CENTRAL EUROPEAN UNIVERSITY

UNFAIR DESIGN PRACTICES AND "THREAT FLAG" SYSTEM AS AN ALTERNATIVE APPROACH TO REGULATION OF DARK UX/UI PATTERNS IN THE EUROPEAN UNION

by Semen Shyshka

LLM Capstone Thesis
SUPERVISOR: Tommaso Soave
Central European University - Private University

June 2023

TABLE OF CONTENTS

ABSTRACT

Over the last decade, the sector of e-commerce has risen dramatically. The reasons for that are not only the development of products and services, but are connected to consumers spending and sharing more due to so-called "dark UX/UI patterns", namely design and interface practices intended to influence consumers' choices for the benefit of e-commerce businesses. After some time, the EU authorities understood the risks associated with such practices and have accordingly adopted or amended various regulations in the field of e-commerce, consumer and data protection. Nevertheless, the regulation remains unclear and fragmentary, whereas its enforcement is non-systematic and often targeted against a particular group of e-commerce businesses.

In response, this thesis proposes an alternative approach to regulation of "dark patterns" in terms of its definition, categorization, and liability of e-commerce businesses for its usage. The methodology of the thesis includes (i-ii) doctrinal legal research simultaneously with policy analysis; (iii) doctrinal and empirical research in the field of IT and psychology; and (iv) comparison of regulatory approaches between the EU and some of other jurisdictions.

The first Chapter of the thesis explains the notion of "dark patterns" and proposes "unfair design practices" (UDPs) as a better legal term. The second Chapter summarizes the EU approach of regulating UDPs and elaborates on its deficiencies mentioned above. The third Chapter proposes an alternative categorization of UDPs depending on the level of threat to consumers, while providing arguments for its usefulness among other taxonomies, and the ways of incorporating the proposals into the current EU legal system.

INTRODUCTION

Over recent years, e-commerce has continued to grow in the European Union, with the proportion of e-commerce consumers among all Internet users in the EU increasing from 55% in 2012 to 75% in 2022.[1] Unfortunately, a considerable part of this increase concerns overconsumption, for instance, when certain practices called "dark patterns" increase users' purchase impulsivity and make them purchase something they did not really want in the first place.[2]

What are "dark patterns"? According to Harry Brignull, a UX designer, who coined this term in 2010, these are features of interfaces and design which make end users do something which they would not have done without those features.[3]

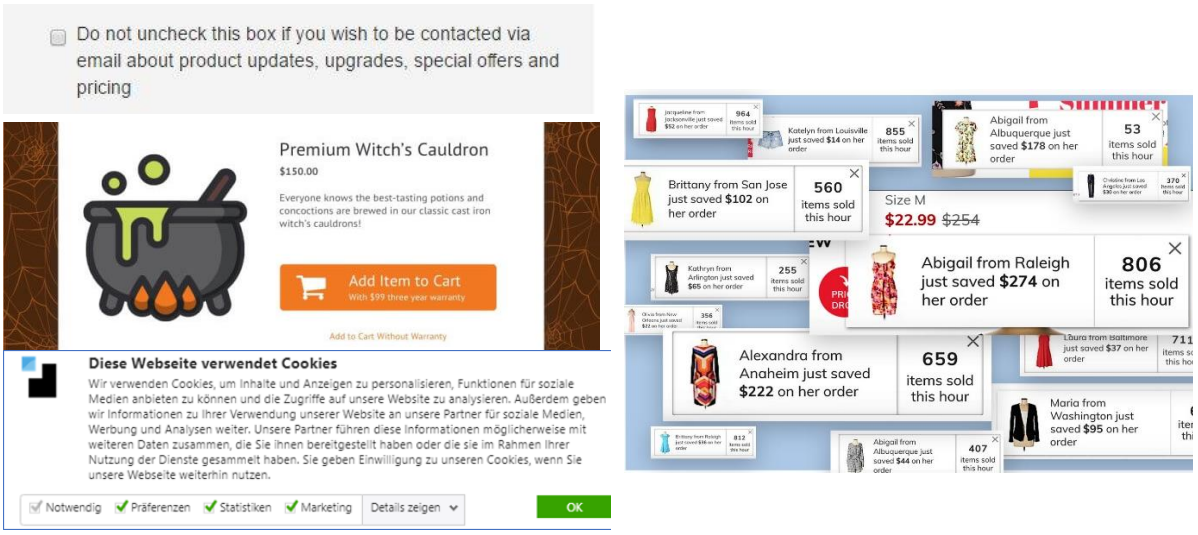
For instance, "sneak into basket" means hiddenly adding small item into the list of other ordered items online; "fake urgency" includes online time-limited proposals for product, which in fact you can purchase after deadline; and "continuous prompting" refers to periodic requests to purchase something or agree to data processing in the product, which you cannot decline once and for all. There are many other dark patterns, examples of which can be found in Figure 1-4 below.

[1] Eurostat, 'E-commerce continues to grow in the EU' (*Eurostat*, 28 February 2023) <https://ec.europa.eu/eurostat/web/products-eurostat-news/w/DDN-20230228-2> accessed 5 April 2023.

[2] Ray Sin et al., 'Dark patterns in online shopping: do they work and can nudges help mitigate impulse buying?' [2022] Behavioural Public Policy, Cambridge University Press 1-27 – p. 23.

[3] Harry Brignull, 'Bringing Dark Patterns to Light' (*Medium*, 6 June 2021) <https://harrybr.medium.com/bringing-dark-patterns-to-light-d86f24224ebf> accessed 5 April 2023.

Figure 1-4. Examples of dark patterns from the Internet: trick question (source - axellescom), false hierarchy (source - Evident), preselection (source - JDSupra), and fake demand (source – NY Times)



Many of above practices can lead to overconsumption among users and make their experience unpleasant, so that businesses become annoying to consumers and lose their trust among their clients.[4] Thus, dark patterns create various harm to consumers, against which there should be effective regulation in the European Union.

Unfortunately, dark patterns kept developing even after being discovered. For instance, *Mathur et al.* discovered at least 1,818 cases of dark patterns in 11k shopping websites in 2019.[5] As regards mobile apps, *Di Geromino et al.* and *Gunawan et al.* found in 2020 and 2021 respectively at least 95% of apps involved in dark patterns with many of them using several

[4] Alex Hill, 'The real impact of dark UX patterns' (*UX Collective, Medium*, 13 January 2022) <https://uxdesign.cc/the-real-impact-of-dark-ux-patterns-fade9d1ca2c6> accessed 5 April 2023; Zipboard, 'Dark Patterns Harm Usability' (*ZipBoard, Medium*, 21 November 2017) <https://blog.zipboard.co/dark-patterns-harm-usability-5b75e293e7a7> accessed 5 April 2023; Maximilian Maier and Rikard Harr, 'DARK DESIGN PATTERNS: AN END-USER PERSPECTIVE' [2020] 16(2) Human Technology 170-199 – p. 186.

[5] Mathur et al., 'Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites' [2019] 3(CSCW), Article 81, Proceedings of the ACM on Human-Computer Interaction, 1-32. – p. 2.

patterns.[6] Finally, lately the European Commission (EC) itself recognized the popularity of dark patterns after (i) finding that 97% of most popular websites/apps used dark patterns and (ii) making separate "sweeps" on particular practices on retail websites.[7] This shows that the problem remains relevant and needs to be solved as soon as possible.

In response to the problem, the EU authorities have adopted various laws in the field of e-commerce, consumer protection, and data protection, including *the General Data Protection Regulation (GDPR)* and *the Omnibus Directive*. While the former strengthens protection against unexpected and unwanted data processing, the latter improved several existing consumer protection directives to, *inter alia*, tackle unfair commercial practices in the form of "dark patterns". [8] The directive was supplemented by updated EC's Guidance, which mentioned the issue of "dark patterns" and how new rules targets them.[9]

At the national level, the authorities of France, Netherlands and Norway have published guidelines that describe their regulation of "dark patterns". [10] In 2021 the Hungarian

[6] Geronimo et al., 'UI Dark Patterns and Where to Find Them: A Study on Mobile Applications and User Perception' [2020] , CHI Conference on Human Factors in Computing Systems 1-14. – p. 1; Gunawan et al., 'A Comparative Study of Dark Patterns Across Mobile and Web Modalities' [2021] 5(CSCW2), Article 377, Proceedings of the ACM on Human-Computer Interaction, 1-29 – p. 16.

[7] European Commission, Directorate-General for Justice and Consumers, Lupiáñez-Villanueva et al., 'Behavioural study on unfair commercial practices in the digital environment: dark patterns and manipulative personalisation: final report' [2002], Publications Office of the European Union – p. 6; European commission, 'Consumer protection: manipulative online practices found on 148 out of 399 online shops screened' (*European Commission*, 30 January 2023) <https://ec.europa.eu/commission/presscorner/detail/en/ip_23_418> accessed 5 April 2023.

[8] Privacy108, 'EU's New Deal for Consumers: a dark future for dark patterns' (*Privacy108*, 24 June 2022) <https://privacy108.com.au/insights/eus-new-deal-for-consumers/> accessed 5 April 2023.

[9] Ecommerce Europe, 'Commission publishes updated guidance documents on the Omnibus Directive' (*ECommerce Europe*, 7 January 2022) <https://ecommerce-europe.eu/news-item/commission-publishes-updated-guidance-documents-on-the-omnibus-directive/> accessed 5 April 2023; Guidance on the interpretation and application of Directive 2005/29/EC of the European Parliament and of the Council concerning unfair business-to-consumer commercial practices in the internal market [2021] OJ 1 526 – section 4.2.7.

[10] CNIL, 'IP Report: Shaping Choices in the Digital World' [2019] 6 Laboratoire d'Innovation Numerique de la CNIL; Autoriteit Consument & Markt, 'IP Protection of the online consumer: Boundaries of online persuasion' (Autoriteit Consument & Markt, 2020); Datatilsynet, 'Digital Services and Consumer Data' (Datatilsynet, 2020).

Competition Authority fined Booking.com EUR 7 million for pressure selling, whereas the French CNIL issued Google and Facebook in total EUR 210 million fines for improperly obtained consent to unnecessary cookies through cookie banners.[11] In certain cases, the EC joined national authorities, so Airbnb made commitments in 2018 to better explain how they present accommodation offers[12] and Amazon agreed in 2022 to facilitate the cancellation process for its Prime membership in the EU.[13]

Finally, in 2022 the European Parliament adopted the Digital Services Act (DSA), which contains a direct ban on dark patterns,[14] while European Data Protection Board (EDPB) has recently finalized its *Guidelines 03/2022 on deceptive design patterns in social media platform interfaces (Guidelines 03/2022)*, which explain which provisions of the GDPR preclude usage of different dark patterns.[15] Hence, the EU authorities have conducted many steps to cover these illegal practices from different angles.

Yet, despite all of the above developments, can one say that the protection against "dark patterns" is now effective? In its *2022 Behavioral study on unfair commercial practices in the digital environment (Behavioral Study)*, the EC itself recognized the ineffectiveness of existing

---

[11] Portfolio, 'Hungary slaps record fine of EUR 7 million on Booking.com' (*Portfolio*, 20 May 2020) <https://www.portfolio.hu/en/business/20200520/hungary-slaps-record-fine-of-eur-7-million-on-bookingcom-432994> accessed 5 April 2023; BBC, 'France fines Google and Facebook over cookies' (*BBC*, 7 January 2022) <https://www.bbc.com/news/technology-59909647> accessed 5 April 2023.

[12] Caitlin Morrison, 'EU cracks down on Airbnb with demands for change in pricing and refund policy' (*Independent*, 16 July 2018) <https://www.independent.co.uk/news/business/news/airbnb-price-refund-policy-eu-compensation-claims-european-commission-a8449546.html> accessed 5 April 2023.

[13] Jon Porter, 'EU forces Amazon to make it easier to cancel Prime subscriptions in Europe' (*Verge*, 5 July 2022) <EU forces Amazon to make it easier to cancel Prime subscriptions in Europe> accessed 5 April 2023.

[14] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) [2022] OJ 2 277 – Recital 67 and Article 25.

[15] European data protection board, 'EDPB publishes three guidelines following public consultation' (*European Data Protection Board*, 24 February 2023) <https://edpb.europa.eu/news/news/2023/edpb-publishes-three-guidelines-following-public-consultation_en> accessed 5 April 2023.

transparency-based remedies and the need for legislative adjustments in the field of dark patterns.[16] Probably this is the key reason why, in 2022, the EC held public consultation called "*digital fairness check on EU consumer law*",[17] while the European Commissioner for justice and consumer protection mentioned "dark patterns" among the topics which the EC might regulate on in the next mandate.[18]

Considering the debates how to improve EU consumer *acquis* related to dark patterns, this thesis proposes an alternative approach to regulation of dark patterns in terms of its definition, categorization, and liability of e-commerce businesses for its usage. Firstly, we should include in the legislation the term "unfair design practices" (UDPs) instead of "dark patterns" because of it being more neutral, inclusive and consistent with existing EU legislation. Secondly, all known dark patterns should be assigned with different "threat flags" based on two criteria (distortion of consumers' behavior and harm caused to consumers). Thirdly, this "threat flag" would be useful for EU and national authorities to provide a proportionate response to illegal activities, and for other stakeholders to be informed of severity of certain practices.

To substantiate this proposal, the thesis deploys (i-ii) doctrinal legal research simultaneously with policy analysis; (iii) doctrinal and empirical research in the field of IT and psychology; and (iv) comparative law methods. The first two methods are useful for

[16] EC Behavioral study, supra note 7 – p. 7.

[17] European commission, 'Digital fairness – fitness check on EU consumer law' (*European Commission*, 17 May 2022) <https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13413-Digital-fairness-fitness-check-on-EU-consumer-law_en> accessed 5 April 2023.

[18] Luca Bertuzzi, 'Dark patterns, online ads will be potential targets for the next Commission, Reynders says' (*Euractiv*, 12 December 2022) <https://www.euractiv.com/section/digital/interview/dark-patterns-online-ads-will-be-potential-targets-for-the-next-commission-reynders-says/> accessed 5 April 2023.

understanding the status-quo of EU system and its drawbacks, while the third and fourth methods help to bring in new regulatory ideas from technical specialists and other jurisdictions.

My argument proceeds as follows. Chapter I elaborates on notion and features of dark patterns and provides arguments for usage of UDPs term. Chapter II summarizes how existing EU regulations and directives address the use of UDPs, and proves why the current EU legal architecture is fragmentary and unclear and does not have an "*effective, proportionate, and dissuasive*"[19] liability system. Chapter III articulates my proposed "threat flags" system, provides a detailed categorization chart, and explains how it can be incorporated into existing EU regulation and used by various stakeholders.

[19] DSA, supra note 14 - Article 52(2).

CHAPTER I: WHAT ARE "DARK PATTERNS" AND WHY SHOULD WE CALL THEM "UNFAIR DESIGN PRACTICES" INSTEAD?

Before deciding *how* to regulate, one should definitely decide *what* to regulate. The concept of "dark patterns" is rather complex and perceived in the public differently. Thus, we need to find (1.1) its key features by analyzing the positions of technical specialists. Based on this analysis and other legal considerations, it is (1.2) proposed to use "unfair design practices" term instead of "dark patterns".

1.1. Meaning and key features of "dark patterns" from non-lawyers' perspective

As mentioned, "dark patterns" include features of web design and interface created to direct users into doing things they were not initially intended to do.[20] These features directed against user are usually based on information asymmetry and cognitive bias.[21] This is because (i) the business have more information about the product and can decide whether and how to present information and (ii) they use such information to cause deviations in our rational thinking and, thus, make us choose less favorable options.

In its *Behavioral Study*, the EC explained that such deviations may arise as a result of (i) misleading, (ii) forcing, (iii) manipulating consumers or (iv) leading them to the decision which is contrary to their interests.[22] For instance, (i) "hidden costs" misleads users about the final price of product by silently adding new charges during checkout process, while (ii) "confirm-shaming" forces user to agree on purchase or other action by presenting refusal options with passive aggression or just negative connotation. With the help of (iii) "price

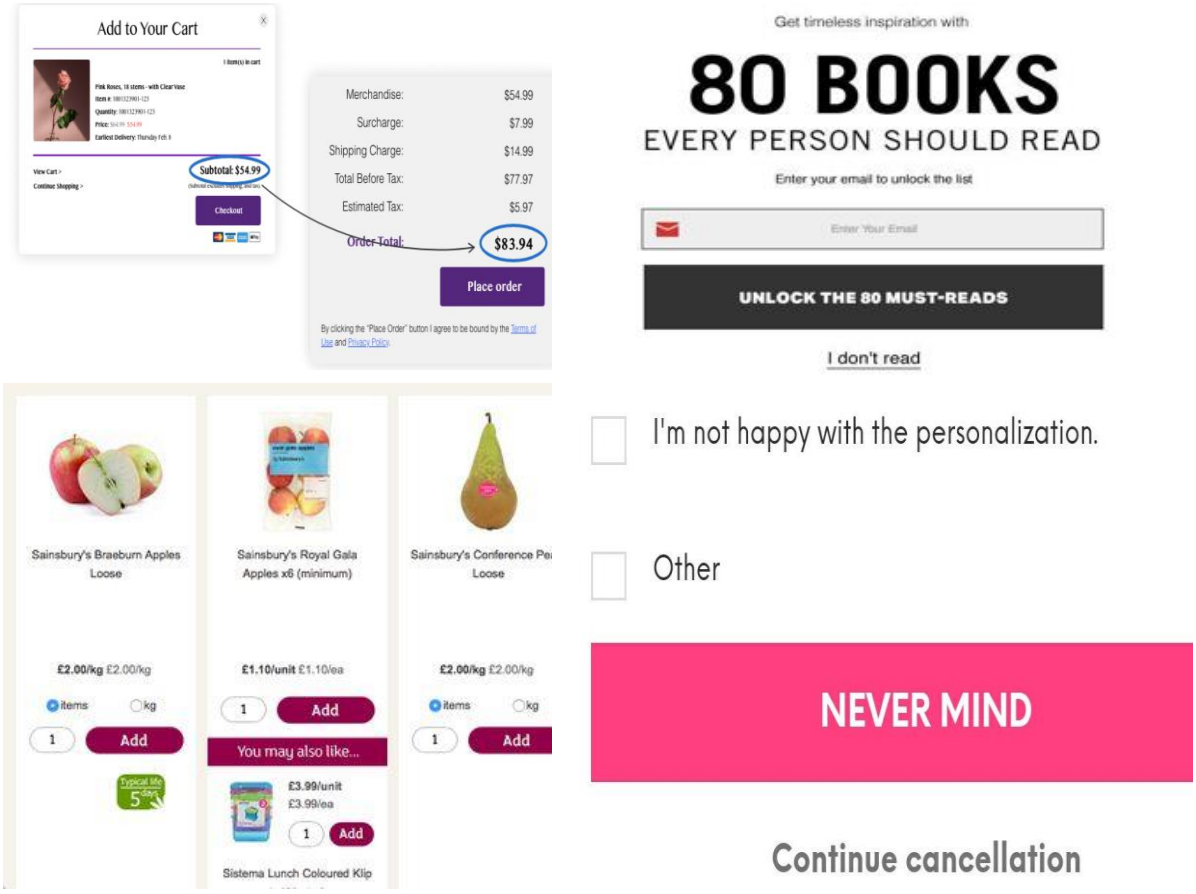
[20] Nerdwriter1, 'How Dark Patterns Trick You Online' (*YouTube*, 29 March 2018) <https://www.youtube.com/watch?v=kxkrdLI6e6M> accessed 5 April 2023.

[21] Chugh et al., 'Unpacking dark patterns: understanding dark patterns and their implications for consumer protection in the digital economy' [2021] 7(1), RGNUL Student Research Review – p. 1, 5.

[22] EC Behavioral study, supra note 7 – p. 20.

comparison prevention", one can manipulate with user's assessment and perception of commercial offer, and (iv) "misdirection" makes users focus on particular information and avoid other choices through, thus leading them to undesired direction.[23]

Figure 5-8. Examples of several dark patterns: hidden costs (source – The Good), confirmshaming (source – UXP Dark Patterns), price comparison prevention (source - mobiversal), misdirection (source – SEOSYDNEY)



Most dark patterns can work differently depending on the circumstances, and there can be other results except for four abovementioned effects on consumers. Still, the key takeaways

[23] Xigen, 'The Dark Patterns Report' (*Xigen*) <https://xigen.co.uk/reports/the-dark-patterns-report/> accessed 5 April 2023.

are the following - dark patterns (i) are introduced as part of design and/or interface of a website or an app and (ii) modify the so called "choice architecture".[24]

Indeed, there are still debates on the scope and features of "dark patterns", including (i) whether intent shall be established, (ii) whether benefit to business or harm to the user shall be assessed, and (iii) whether dark patterns shall be deceptive or not.[25]

Section 3.1 contain my own views on these topics in order to make EU regulation more efficient. As for now, I may briefly conclude that (i) intent is not *conditio sine qua non* for dark patterns, and it is better to clearly explain to stakeholders what is prohibited instead of analyzing fault of designers; (ii) the harm to end users is more important criterion, because regulation shall protect consumers instead of simply restricting e-commerce; and (iii) dark patterns do not only deceive people, so we need to include aggressive practices in the notion.

1.2."Unfair design practices" as more neutral, inclusive, and consistent legal term

There is an old saying "*As you name the boat, so shall it float*", which definitely applies not only to ships but legal concepts. The more thoroughly one creates the name and definition of certain practice, the easier would be to understand it and use this definition for emerging practices not directly regulated before.

In this regard, the starting proposal in this thesis is to rename "dark patterns" into "unfair design practices" (UDPs) as design and interface commercial practices, which materially causes or is likely to cause average consumer to take otherwise unwanted decision and/or not

[24] Mathur et al., 'What Makes a Dark Pattern... Dark? Design Attributes, Normative Considerations, and Measurement Methods ' [2021] Proceedings of the CHI Conference on Human Factors in Computing Systems, 1-18 – p. 5.

[25] Mathur et al., 'Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites' [2019] 3(CSCW), Article 81, Proceedings of the ACM on Human-Computer Interaction – pp. 2-3.

take desired decision. There are three arguments for using the new term at least in the EU jurisprudence.

Firstly, the existing term is not descriptive, because there is no reference to design and interface as well as the word "dark" does not explain the features of these practices. There are various ranges of threats for consumers created by dark patterns and some of practices stay on the thin line between legitimate persuasive marketing and manners of manipulation.[26] Leaving the status quo might lead authorities to create many shades of "grey patterns" to distinguish completely prohibited practices with something being "on the line". Probably this was one of the main reasons why Harry Brignull and the EDPB switched from "dark patterns" to use of "deceptive design (patterns)".[27]

Secondly, using UDPs term would be more consistent with the EU law than both "dark patterns" and "deceptive design (patterns)". Pursuant to UCPD's concept of unfairness, there is prohibition on misleading, aggressive and those practices being contrary to professional diligence, [28] while "deceptive" term covers only misleading claims. Considering that there are many manipulations not strictly connected with deceiving consumers (such as confirm-shaming, forced registration or continuity, etc.), usage of "unfair" instead of "deceptive" would

[26] Jennifer Riggins, 'Critics of 'Deceptive Design' Push for a More Ethical UX' (*The New Stack*, 11 March 2022) <https://thenewstack.io/critics-of-deceptive-design-push-for-a-more-ethical-ux/> accessed 5 April 2023; System Concepts, 'Persuasive design vs dark patterns: Where to draw the line' (*System Concepts*, .) <https://www.system-concepts.com/insights/persuasive-design-vs-dark-patterns/> accessed 5 April 2023; Laura Lugo, 'Deceptive Design and how to avoid dark patterns' (*Bootcamp*, *Medium*, 30 June 2022) <https://bootcamp.uxdesign.cc/deceptive-design-and-how-to-avoid-dark-patterns-62a6dff026e4> accessed 5 April 2023.

[27] Harry Brignull, 'About this site' (*Deceptive Design*) <https://www.deceptive.design/about-us> accessed 5 April 2023; European Data Protection Board, Guidelines 03/2022 on Deceptive design patterns in social media platform interfaces (European Data Protection Board 2023) – p. 8.

[28] Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council (Unfair Commercial Practices Directive) [2005] OJ 2 149 – Article 5.

be in line with existing terms in the EU law. Also, the word "practices" as action/omission or course of such acts would be better than "pattern" as design or repeated arrangement, since the dark patterns may consist of (i) single one action/omission (for example, fake review or hidden charges) or (ii) set of such acts (for instance, "hard to cancel" or friend spam).

Thirdly, there were recent discussions that the term "dark patterns" is harmful to people of color, because it perpetuates the long-standing perception of dark/black as a negative color.[29] The proposed UDPs term would be a neutral alternative to "dark patterns", because the word "unfair" neither refers to any category of people nor creates perception that someone is better or worse.

Therefore, one should use UDPs instead of "dark patterns" term because of it being more neutral, inclusive, and consistent with the EU law. Nevertheless, all features of UDPs that are recognized by UX specialists, such as the use of design&interface and modification of choice architecture, shall remain in the definition.

[29] Caroline Sinders, 'What's In a Name? Unpacking Dark Patterns versus Deceptive Design' (*Medium*, 18 June 2022) <https://medium.com/@carolinesinders/whats-in-a-name-unpacking-dark-patterns-versus-deceptive-design-e96068627ec4> accessed 5 April 2023; Todd Libby, 'Enough with "Dark Patterns" Already! This Isn't Going To Go Over Well' (*Todd Libby*, 1 January 2023) <https://toddl.dev/posts/enough-with-dark-patterns-already/> accessed 5 April 2023; Amy Hupe, 'Why it's time to update our language about bad design patterns' (*Amy Hupe*, 1 July 2022) <https://amyhupe.co.uk/articles/changing-our-language-on-bad-patterns/> accessed 5 April 2023.

CHAPTER II: WHAT IS THE CURRENT EU ARCHITECTURE OF REGULATING UNFAIR DESIGN PRACTICES AND WHY IS IT NOT EFFICIENT?

Before explaining changes to the EU legislation and their necessity to the society, one should understand (2.1) how the EU currently deals with UDPs with the help of regulations and directives. Afterwards, there are two critiques presented on current legislation, namely (2.2) the fact of EU regulation against UDPs being fragmentary and unclear and (2.3) unsystematic application of administration fines against e-commerce businesses for the use of UDPs. Resolving these problems serves as regulatory objectives, which are taken into account for proposal of changes in EU legislation in Chapter III.

2.1. Regulatory response to "unfair design practices" in the European Union

Since UDPs may affect consumers in many fields, including choice of the product/service and personal data sharing, there are many acts in the EU law which either directly prohibit UDPs or establish requirements adherence to which precludes usage of the practices. As the goal of this Section is to briefly explain the general framework, the analysis will be restricted to acts of wide applicability, thus excluding sector-oriented acts. Accordingly, it is sufficient to review (2.1.1) consumer protection directives updated by the Omnibus Directive (*UCPD, Consumer Rights Directive (CRD), Unfair Contract Terms Directive (UCTD), and Price Indication Directive (PID)*), (2.1.2) data protection regulations and directives (*GDPR and ePrivacy Directive*), and (2.1.3) general e-commerce acts (*DSA, e-Commerce Directive, and Digital Market Act (DMA)*).

2.1.1. Consumer protection directives

The vast majority of anti-UDP obligations are hidden in several consumer protection directives, especially in the UCPD. This directive protects against both misleading and

aggressive acts as a part of B2C commercial practices, while remaining supplementary to obligations in sector-oriented EU acts.[30] It contains a non-exhaustive list of presumptively unfair practices in Annex I, which includes bait and switch, limited availability with fake timers and limited stock claims, fake reviews, fake winning of prize; but EC also recognized that other practices are covered, such as misleading free trials and subscription traps, double negative questions, drip pricing, etc.[31]

The remaining UDPs may also be covered by UCPD provided they materially distort the economic behavior of consumer by making him click on the advertisement, purchase the product/service, or spend more time on specific platform, etc.[32] This can be confirmed through positions of French and Dutch DPAs, which described dark patterns as user interface designed to cause consumer to make unwanted decisions (with Dutch DPA stating that "*dark patterns can constitute unfair commercial practices*").[33] In the UK, authorities described "dark patterns" just as one of the types of harmful online choice architecture (OCA) practices (apart from sludge and dark nudges). Still, they impliedly admit their relevance to "unfair commercial practices" through mentioning UK BEIS's proposal to include some of dark patterns in Schedule 1 to *the Consumer Protection from Unfair Trading Regulations*.[34]

As opposed to UCPD, most requirements under CRD are related to provision of information on business, product/services, its characteristics, price, other important contract

[30] UCPD, supra note 28 - Articles 2(d), 3(4), 6-8; UCPD Commission Guidance, supra note 9 – section 1.2.1.

[31] UCPD, supra note 28 - Annex I, items 6, 7, 8, 19, 23b, 23c; UCPD Commission Guidance, supra note 9 – sections 2.9.6, 4.2.4, 4.2.7, and 4.2.8.

[32] UCPD, supra note 28 - Articles 2(e) and 5; UCPD Commission Guidance, supra note 9 – section 2.4.

[33] CNIL Report, supra note 10 – p. 34; ACM Guidance, supra note 10 – p. 52.

[34] Department for Business, Energy, and Industrial Strategy (BEIS), Reforming Competition and Consumer Policy (2021) – p. 94, para. 2.45.

terms, etc.[35] Still, it interplays a lot with (i) UCPD in precluding ambiguous prices, hidden subscription, mention of important information in terms and conditions only, overloading user with unstructured information and (ii) Article 6a UCPD in requirement for proper calculation of discount and prohibition to make "forever sales".[36]

Finally, UCTD prohibits various unreasonable B2C contract terms, which can be used as supportive instrument for achievement of certain UDPs. For instance, UCTD can protect against subscription traps (when contracts have automatic extension subject to expressing desire not to extend unreasonably in advance) or hidden charges (when agreement allows to change the price with no right for consumer to cancel).[37]

2.1.2. Data protection legislation

GDPR and ePrivacy Directive substantially influences the processing personal data of EU residents, including through a range of obligations directly or indirectly targeted against UDPs. Firstly, there are lots of personal data processed under "consent" legal basis (for ePrivacy Directive – any data for direct marketing and not strictly necessary cookies[38]), but the proper consent needs to be through affirmative act, informed, freely given and distinguishable

[35] Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council [2011] OJ 2 304 - Articles 6 and 8.

[36] *Ibid*; Guidance on the interpretation and application of Directive 2011/83/EU of the European Parliament and of the Council on consumer rights [2021] OJ 1 525 – sections 3.1.2, 3.2.3, and 4.2.2.

[37] Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts [1993] OJ 2 095 – Annex I, items 1(h), (j), and (l).

[38] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) [2002] OJ 2 201 – Articles 5(3) and 13(1).

from other matters, and users shall have ability to withdrawn easily at any time.[39] This means that, for example, preselection (pre-ticked boxes), continuous prompting (asking users to consent until they agree), confirm-shaming (forcing users to "consent" by presenting "reject" as rather negative option), trick questions (ambiguous information on purposes of processing or with double negatives in sentence)[40] are definitely prohibited, since they lead to unlawful processing without proper legal basis.

Secondly, Article 5 sets out key principles of data processing, where the principle of fair processing stands out. In EDPB's opinion, this principle serves as a starting point to define whether there was detrimental, misleading, discriminatory or unexpected data processing, which may serve as evidence of using "deceptive design patterns".[41]

Thirdly, the GDPR contains some more detailed obligations to respect user's data, for instance, exercise of data subjects' right or transparency during data collection. In turn, compliance with this obligation precludes usage of UDPs, where businesses deceive user about data deletion (deceptive snugness) or provide ambiguous or inconsistent information about data processing ("left in dark").[42]

2.1.3. General e-commerce acts

Finally, DSA provides the first and only direct prohibition to creating online interfaces which deceive, manipulate consumers, or materially distort their ability to make free and

[39] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ 2 119 – Recital 32 and Article 7.

[40] EDPB Guidelines 03/2022, supra note 27 - p. 18, para. 33; p. 19, para. 43; p. 24, para. 60; p. 28, para. 73.

[41] European Data Protection Board, Guidelines 4/2019 on Article 25 Data Protection by Design and by Default (European Data Protection Board 2020) – p. 16.

[42] EDPB Guidelines 03/2022, supra note 27 – p. 52, para. 149; p. 56, para. 157

informed choices.[43] However, it applies (i) only to providers of intermediary services (for instance, search engines, social media, marketplaces, etc.) with the exclusion of micro and small enterprises, and (ii) does not cover the practices already covered by UCPD and GDPR.[44]

As opposed to DSA, DMA apply only to "gatekeepers" with more than EUR 7,5 million annual turnover for 3 years or 45 million monthly active users.[45] The act consists of some rules (for instance, prohibition to force users of one activities to subscribe to other activities or requirement for applying fair and transparent rankings)[46] that are also intended to avoid undue influence through UDPs.

Unlike DSA and DMA, e-Commerce Directive applies to all online businesses, but contains much less requirements related to UDPs. In particular, the businesses have to provide such information, as (i) their contact details as well as (ii) clear and unambiguous prices and conditions for their products/services and commercial offers.[47] This in turn may preclude businesses from price comparison prevention, hidden charges, sneak into basket (because price needs to be disclosed clearly) or "hard to cancel" (as consumer will use your published contact details to ask for cancellation).

As a result of review of regulations and directives related to UDPs, one can summarize the EU legal architecture on this topic with the help of below chart.

[43] DSA, supra note 14 – Article 25.

[44] *Ibid.* – Articles 19(1) and 25(1).

[45] Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) [2022] OJ 2 265 – Article 3.

[46] *Ibid.* - Articles 5 and 6.

[47] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce') [2000] OJ 2 178 – Articles 4 and 5.

Chart 1. Overview of the key EU regulations and directives in the field of UDPs: applicability, relevant obligations and potentially covered UDPs.

EU Legal Act	Applicability for Businesses & Activities	Types of Key Obligations in the Act	Types of UDPs Potentially Covered
		Key acts against UDPs	
UCPD	Businesses involved in B2C relationships before, during and after conclusion o the contract	1)Abstract prohibition of unfair commercial practices, where misleading and aggressive are types, but not exhaustive ones (Art. 5) 2)Also general prohibition of misleading actions and omissions and aggressive actions (also of them – extensive prohibition of influence) 3)Finally – there is non-exhaustive Annex I of activities	1)Can potentially cover all UDPs 2)Definitely covers the following: • a)bait advertising and bait and switch; • b)limited offers; • c)hidden recommended system; • d)fake prize and fake free; • e)non-verified and fake reviews; f)exhortation to children;
DSA	Intermediary services (mere conduit, caching, hosting). Some obligations are excluded for micro/small enterprises.	1)Direct prohibition of UDPs (Art. 25); 2)Prohibition of other influence: • No profiling for ads with special category (Art. 26); • Allowing to change recommender system (Art. 27) → at least one option not based on profiling (Art. 38). 3)Information requirements: • Disclosure of advertising (Art. 26); • Clear terms and conditions (Art. 14); Parameters for recommender system (Art. 27)	1)All UDPs except those regulated by UCPD and GDPR 2)Some UDPsrelated with ToS, advertising and recommendations
GDPR	Everyone who processes data of EU residents *(when EU resident OR directs activities to EU residents*)	1)Prohibition of influence: • Conditions of general consent (Art. 7) • Prohibition on processing of special category (Art. 9) • Right to delete or object processing, including profiling (Art. 17+21) 2)Abstract requirements (Art. 5) • Lawfulness, fairness and transparency of data processing (+ grounds for processing – Art. 6) • Purpose limitation and Data minimization 3)Information requirements: • Transparency through PP and during collection (Art. 12-13)	1)UDPs forcing users to share personal data or not allowing them to do something with collected data 2)UDPs related to oversharing by default, cookie banners, confirm-shaming or other forced consent, misleading info about processing, impossibility to easily do something with data

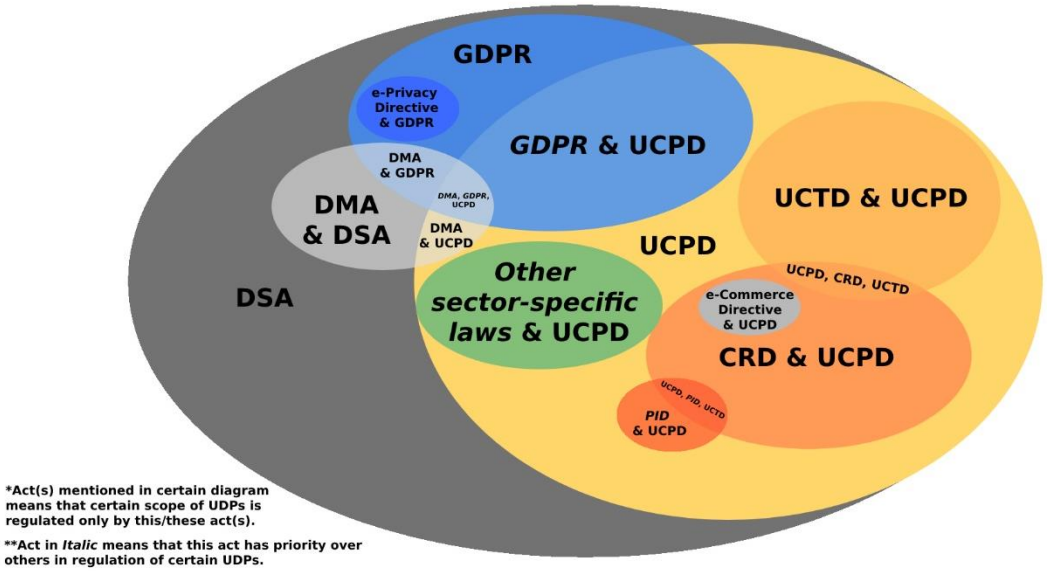
		• Notifications on data deletion (Art. 19) 4)Additional protection to minors → Conditions of consent of minors (Art. 8)	
ePrivacy Directive	Everyone involved in public electronic communications	1)Other compliance obligations: • Need to obtain consent for all cookies and tracking technologies, except those strictly necessary (Art. 5) • Strictly necessary cookies needs to be used only for strictly necessary purposes without consent (Art. 5) • Opt-in for direct marketing through emails (Art. 13) When you have prior relationships – soft opt-in with right to opt-out during data collection at each email (Art. 13)	Preselection, hidden information, confirm-shaming, disguised ads, trick questions, etc.
Supporting acts in the field of consumer protection			
CRD	Businesses involved in B2C relationships before, during and after conclusion of the contract	1)Prohibition of influence: • Information from Arti. 6(1) cannot be altered unless parties expressly agreed otherwise (Art. 6) • Obligation to pay shall be explicitly mentioned (Art. 8) • Clearly disclosing waive of withdrawal rights if any (Art. 16) 2)Information requirements: • Need to provide range of information in clear and comprehensible manner before conclusion of contract (Art. 6) • Need to provide specific info for marketplaces (Art. 6a) • For distance contract – at least need to mention in clear and prominent manner before obligation to pay → main characteristics, price, duration of contract and minimum duration of consumer's obligations (Art. 8)	1)UDPs related to providing incorrect information or hiding it, including disclosure on subscriptions (price comparison prevention, roach motel, sneak into basket, hidden information, hidden costs, etc.)
PID	Businesses involved in B2C relationships before and during conclusion of the contract	1)Information requirements on proper indication of prices and discounts (Art. 6a)	1)UDPs related to indication of price (Price comparison prevention, hidden information, hidden costs, etc.)
UCTD	Businesses involved in B2C relationships (aspects related to contract terms itself)	1)Prohibition of influence → prohibition of unfair terms (Art. 3-4) → non-exhaustive list of unfair terms in Annex 2)Information requirement → need to present contracts in plain and intelligible language (Art. 5)	Certain terms may be part of dark patterns: • b)Changing price with no right to cancel; • c)Too early necessity to forbid extension of contract; • d)Putting new unpredictable terms;

			e)Alteration of contract without valid reason
Supporting acts in the field of e-commerce			
DMA	Only to gatekeepers with EUR 7,5+ billion annual turnover for last 3 years or 45 million monthly active end users, who perform "core activities" (search engines, intermediation, social networking, etc.)	1)Prohibition of influence: • Not requesting "opted-out" users to consent more than once a year (Art. 5) • Cannot require to register with or subscribe to other core activities as a condition to use intended core activities (Art. 5) • Not treating own products more favourably (through indexing/crawling, etc.) by applying transparent, fair and non-discriminator ranking (Art. 6) 2)Abstract requirements → necessity to comply with above obligations through different measures, which also comply with consumer protection legislation (Art. 8)	Continuous prompting, hidden information, roach motel, etc.
E-Commerce Directive	All e-commerce business (if EU law apply)	1)Information requirements: • General info about company on website/app (Art. 5); • Clear and unambiguous prices (Art. 5); • Clear explanation of commercial communications, including grounds for certain offers (Art. 6).	Intermediate currency / price comparison prevention, hidden information, fake limit/urgency, etc.

2.2. Unclear and fragmentary nature of the EU substantive obligations against UDPs

As can be seen on the above chart from Section 2.1, the current EU system of UDPs remains rather fragmentary. This is because many acts cover the same dark pattern in different or sometimes the same ways, and only in several cases one of the acts take the priority over another one (practices which are covered by several acts were highlighted in red in Chart 1 above). The interplay of most relevant EU acts is presented in the below chart, where the biggest ellipse represents all UDPs and other ellipses show how different acts cover part of UDPs.

Chart 2. Diagram showing how EU acts interplay with each other in regulation of UDPs



According to above chart, the considerable part of UDPs is already covered by several acts with no priority over each other, which makes it unclear for stakeholders which particular acts may apply to the certain practice and the risks of double jeopardy issues.

Even if we assume that governmental agencies always comply with *ne bis in idem* principle, there is serious lack of clarity on interplay between three key acts related to UDPs, namely the DSA, UCPD, and GDPR. As mentioned above, the DSA only covers those practices which are not covered by the DSA and GDPR.[48] However, the concept of "unfairness" under UCPD theoretically allows to cover all UDPs related to transactional decision of consumer (which is interpreted widely), while fair processing and other principles of data protection under GDPR also can be helpful in assessment of legality of certain practices related to consumers' personal data.

[48] DSA, supra note 14 - Article 25(2).

Considering that, under EC's opinion, UCPD works as a "safety net" to other sector-specific EU legislation,[49] the DSA operates just as a "safety net for the safety net" with no clear understanding among stakeholders of its scope. And if the regulators would not make proper distinction between simply persuasive techniques and dangerous design and interface, everything could be treated as UDPs and, hence, nothing would be actually UDPs.[50] Probably for this reason *BEUC* recommended the EC to provide guidance to companies on legal boundaries on such persuasion techniques and the ways to avoid UDPs in designing the website.[51]

2.3. Lack of "*effective, proportionate and dissuasive*" penalties for "unfair design practices" in the European Union

There are also issues with enforcement of such obligations, including through proper penalties against infringers. The below chart summarizes the range of possible fines under EU legal acts related to UDPs and the criteria, which shall be used by the enforcement bodies and courts in the course of assessing the amount of fines.

Chart 3. Overview of applicable penalties and assessment criteria in the EU regulations and directives in the field of UDPs

EU Legal Act	Range of Fines	Liability Criteria
Key acts against dark patterns		
UCPD	Fines (Art. 13): • At least 4% of the trader's turnover in Member States for the last year or at least EUR 2 million;	**Effective, proportionate, dissuasive** (Art. 13) Criteria (Art.13) • Nature, gravity, duration • Scale • **Mitigation of damages**

[49] UCPD Commission Guidance, supra note 9 – section 1.2.1.

[50] Catalina Coanta and Cristiana Santos, 'Dark Patterns Everything: An Update on a Regulatory Global Movement' [2023] Network Law Review <https://www.networklawreview.org/digiconsumers-two/> accessed 28 May 2023.

[51] BEUC, "DARK PATTERNS" AND THE EU CONSUMER LAW ACQUIS (BEUC 2022) – p. 12.

	• States may limit fines to breaching Art. 6-9 UCPD or continued use of other unfair commercial practices.	• Previous infringements • Financial benefits gained or losses avoided • Penalties for same cases in other jurisdiction • **Any other aggravating or mitigating factors applicable.**
DSA	Usual fines (Art. 52+74) • Almost all - up to 6% of worldwide turnover for last year; • When providing incorrect information to supervisor - up to 1% of worldwide turnover for last year. Periodic payments (Art. 52+76) → up to 5% average daily worldwide turnover in last year per day	**Effective, proportionate, dissuasive** (Art. 52) Criteria (Art. 74) • Nature, gravity, duration; • Recurrence.
GDPR	Usual fines (Art. 83): • Failure of parental consent – up to EUR 10 mln or 2% of worldwide turnover for last year, whichever is higher; • Violation of DP principles, grounds for processing, "proper" consent, processing of special category – up to EUR 20 mln or 4% worldwide turnover for last year, whichever is higher; • Lack of transparency, not allowing to erase data or decision through automated means – same fine as above.	**Effective, proportionate, dissuasive** (Art. 83) Criteria (Art. 83) • Nature, gravity, duration; • Intentional or negligent character • **Mitigation of damages** • Degree of responsibility • Previous infringements • Categories of affected data • If notified supervisors • Compliance with previous interim measures • Adherence to code of conducts / certifications • **Any other aggravating or mitigating factor**
ePrivacy Directive	*NO DETAILS*	**Effective, proportionate, dissuasive** (Art. 15a
Supporting acts in the field of consumer protection		
CRD	Fines (Art. 24) → At least 4% of of the trader's turnover in Member States for the last year or at least EUR 2 million.	**Same as for UCPD** (Art. 24)
PID	*NO DETAILS*	**Effective, proportionate, dissuasive** (Art. 8)
UCTD	Fines (Art. 8b) → At least 4% of of the trader's turnover in Member States for the last year or at least EUR 2 million.	**Same as for UCPD** (Art. 8b)
Supporting acts in the field of e-commerce		
DMA	Usual fines (Art. 30) • Up to 10% worldwide turnover for the last year; • If repeated within 8 years (and confirmed earlier by non-compliance decision) – up to 20% worldwide turnover for the last year. Periodic payments (Art. 31) → up to 5% average daily worldwide turnover in last year per day.	Criteria (Art. 30) • Gravity, duration • Recurrence

eCommerce Directive	*NO DETAILS*	**Effective, proportionate, dissuasive** (Art. 20)

Based on the above chart, almost each of the EU legal acts related to UDPs requires penalties to be "effective, proportionate and dissuasive". But does this statement of requirement really change the situation? In my opinion, (i) the above ranges of fines are sometimes not proportionate to the type of practices covered by each regulation or directive. Moreover, (ii) the existing criteria for calculation of fines do not properly address the seriousness of each UDP, which (iii) leads to inconsistencies in decisions of governmental agencies.

First and foremost, the potential liability under different regulations differs substantially, namely with consumer protection directives providing up to 4% of EU annual turnover or EUR 2 million and DMA establishing fines up to 20% of worldwide annual turnover for repeated infringements. While it is true that "liability caps" were established taking into account the type of businesses subject to fines (every e-commerce for CP directives, but only big intermediaries and "gatekeepers" for DSA and DMA respectively) or things affected by UDP (personal funds, privacy or market integrity, etc.), this still do not provide proportionate response to existing deceptive designs.

For instance, many practices that successfully "distort consumer behavior" (such as fake reviess, hidden charges, etc.) were already recognized as dangerous and, thus, prohibited by Annex I of UCPD.[52] At the same time, many of "weak" UDPs, still not recognized by UCPD and GDPR, will be governed by DSA and, accordingly, may be paradoxically punished with higher fines (up to 6% of worldwide annual turnover) despite them possessing lesser threat to community than those listed in Annex I.

[52] UCPD, supra note 28 – Annex I, items 20, 23b, 23c.

Secondly, the existing liability criteria are also not appropriate, with eCommerce Directive and ePrivacy Directive providing no criteria and DSA and DMA mentioning only 4 general criteria. Consumer protection directives and GDPR use penalty criteria similar to DSA&DMA and add several other factors, but none of them help to differentiate the level of threat posed by each UDP.

The opponents could mention so called "gravity" criterion being present in most of the EU legal acts related to UDPs, but *EDPB Guidelines 04/2022 on the calculation of administrative fines under the GDPR* shows that this criterion operates differently.[53] In particular, EDPB proposes to consider the circumstances of the processing, its scope, and the number of the harm caused to consumers.[54] While such criteria can be used for assessment of illegal processing (which can be one of the results of UDPs), it does not help evaluate UDPs itself without referring to individual situations each time.

Thirdly, one can indeed mention that the EDPB proposes starting amounts, namely 0-10%, 10-20%, and 20-100% of maximum GDPR fine, depending on the level of breach,[55] whereas the Dutch DPA and the conference of German regional DPAs established sub-ranges of penalties depending on the level of breach and infringer's turnover.[56] However, the below

[53] European Data Protection Board, Guidelines 04/2022 on the calculation of administrative fines under the GDPR (European Data Protection Board 2023).

[54] *Ibid.* - pp. 16-17, paras. 52 – 54(a-c).

[55] *Ibid.* – p. 19, para. 61.

[56] Autoriteit persoonsgegevens, Beleidsregels van de Autoriteit Persoonsgegevens van 19 februari 2019 met betrekking tot het bepalen van de hoogte van bestuurlijke boetes (Boetebeleidsregels Autoriteit Persoonsgegevens 2019) (Staatscourant 2019) – pp. 1-2; Konferenz der unabhängigen datenschutzaufsichtsbehörden des bundes und der länder, Konzept der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder zur Bußgeldzumessung in Verfahren gegen Unternehmen (Datenschutzkonferenz 2019) – pp. 3-8.

evidence of data protection and consumer protection cases suggests that in practice EU Member States differently analyze and calculate the fines for UDPs.

As regards data protection cases, in *CNIL (France) vs Facebook* there was a practice of placing "cookie-banner" with a confusing "accept cookies" button, and the CNIL fined Facebook with EUR 60 million for that in 2021. Despite the serious amount of penalty, there was not much discussion on the gravity of the "cookie-banner" itself, and the French regulator mostly focused on Facebook's turnover and cookies being crucial part of its business model.[57] A similar situation arose in *APD/Gegevensbeschermingsautoriteit (Belgium) vs Rochel&Sie* (inappropriate consent to cookies based on "further browsing" technique), where the Belgian DPA rather briefly explained the so-called "*nature, gravity and duration of the infringement*" to impose EUR 50,000 fine.[58] In *Garante (Italy) vs Ederson Energia* (misleading consumers to use their data for direct marketing and profiling purposes) the Italian authorities considered number of affected users, negligence and company's turnover to adopt EUR 4,9 million fine, but again avoided discussion on harm of particular UDPs.[59]

Overall, the above cases show that GDPR is enforced differently against UDPs in each Member State, both in terms of choosing the reasons for calculation of appropriate fine and the way of describing such reasons.

[57] CNIL Restricted Committee, 'Deliberation of the restricted committee No SAN-2021-024 of 31 December 2021 concerning FACEBOOK IRELAND LIMITED' (*CNIL*, 31 December 2021) <https://www.cnil.fr/sites/default/files/atoms/files/deliberation_of_the_restricted_committee_no._san-2021-024_of_31_december_2021_concerning_facebook_ireland_limited.pdf> accessed 28 May 2023. – pp. 19-20.

[58] Autorite de protection des donnees Gegevensbeschermingsautoriteit, 'Décision quant au fond 103/2022 du 16 juin 2022' (16 June 2022) <https://www.autoriteprotectiondonnees.be/publications/decision-quant-au-fond-n-103-2022.pdf> accessed 28 May 2023. – para. 107.

[59] Garante per za Protezione dei Dati Personali, ' Provvedimento inibitorio, prescrittivo e sanzionatorio nei confronti di Edison Energia S.p.A. - 15 dicembre 2022 [9856345]' (15 December 2022) < https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9856345> accessed 28 May 2023. – section 5.

With respect to consumer protection cases, in *ACGM (Italy) vs Ryanair* (nudging consumers to obtain vouchers through provision of incorrect information on cancelled flights during COVID-19) the authorities again analyzed the seriousness of the breach based on turnover, number of affected users, harm to them, and financial benefits from practice.[60] In the meantime, in *GVH (Hungary) vs Booking.com* (fake limited availability claims and misleading "free cancellation" statements) and *ACM (Netherlands) vs TrendX* (incorrect delivery terms and fake online reviews) the governmental agencies took into account their fine policies with sub-ranges of penalties.[61] Nevertheless, in those cases agencies also mostly looked not on seriousness of each UDP itself, but on overall harm caused by the commercial practice against consumers.

Hence, it is necessary to have new detailed criteria with severity of each UDP, which is proposed in this thesis. Firstly, it would unite all common UDPs despite their affiliation with purchasing, data sharing or other related fields. Secondly, it would provide clarity to stakeholders about which design practices are illegal and to what extent. Finally, the proposed chart would serve as a good "starting point" for proportionate assessment of fines.

[60] Garante della Concorrenza e del Mercato, ' PS11865 - RYANAIR/CANCELLAZIONE VOLI POST-COVID' (11 May 2021) < https://www.agcm.it/dotcmsCustom/tc/2026/5/getDominoAttach?urlStr=192.168.14.10:8080/C12560D000291394/0/54CACC5C721669EBC12586DF00532F03/$File/p29665.pdf > accessed 28 May 2023. – paras. 143-153.

[61] Gazdasági Versenyhivatal, 'Határozatot a Booking.com ellen' (2018) < https://gvh.hu/pfile/file?path=/dontesek/versenyhivatali_dontesek/versenyhivatali_dontesek/dontesek_2018/vj017_2018_m&inline=true > accessed 28 May 2023; ACM, ' Decision of the Netherlands Authority for Consumers and Markets regarding the imposition of a fine on TRENDX B.V' (2022) < https://www.acm.nl/system/files/documents/decision-fine-trendx.pdf > accessed 28 May 2023.

CHAPTER III: HOW CAN A "THREAT FLAG" SYSTEM IMPROVE THE EXISTING LIABILITY SYSTEM?

There are various ways in which the existing regulation of UDPs can be improved, and it is up to EU authorities and Member States to decide which legal form it should take. The goal of this thesis (and Chapter III in particular) is to provide alternative conceptual view on UDPs, which would help to make regulation unitary, legal consequences – clear, and administration fines – proportionate. Under this view, there must be alternative categorization of different UDPs into green/yellow/orange/red flags based on their level of the threat, which would be used by all stakeholders in assessing the "harmfulness" of business practices and the amount of penalties.

The idea for assessment of "harmfulness" of dark patterns was inspired by works of such specialists, as *Mathur et al.*, *Nyström and Stibe*, and *Nagda*.[62] However, my proposal differs because of desire to incorporate the new categorization into the "legal world". The use of the notion of "flags" to evaluate harmfulness was taken from the investment and consulting industries, where investors and auditors often describe problems with the help of yellow (usual problem) and red flags (serious problem).[63] By transposing these terms from due diligence processes to day-to-day e-commerce activities, the categorization would create better association of certain UDPs as "really warning" or "cautionary". In turn, this would give better

[62] Mathur et al, 2019, supra note 25 – p. 79; Tobias Nyström and Agnis Stibe, When Persuasive Technology Gets Dark?. in Themistocleous and others (eds), Information Systems: 17th European, Mediterranean, and Middle Eastern Conference (Springer 2020); Yashasvi Nagda, 'What is Darkness in Dark Patterns?' (Medium (Muzli - Design Inspiration), 17 March 2020) <https://medium.muz.li/what-is-darkness-in-dark-patterns-e981465c0c57> accessed 28 May 2023.

[63] Adam Hayes, 'What Is a Red Flag? Definition, Use in Investing, and Examples' (*Investopedia*, 25 March 2022) <https://www.investopedia.com/terms/r/redflag.asp> accessed 28 May 2023; Nick Killick, ' From Red to Green Flags' (*IHRB*, 2 May 2011) <https://www.ihrb.org/focus-areas/commodities/commentary-red-green-flags-corporate-responsibility> accessed 28 May 2023.

understanding for consumers that they should avoid using services with “red flag” practices, and for investors that they should avoid making investments in such high-risk companies.

The ”threat flag” shall be established based on two criteria – (i) the level of distortion in consumers’ behavior which is caused by the relevant UDP and (ii) the level of harm such UDP causes to individual consumer. These criteria were based on both proposals/case studies of human-computer interaction (HCI /CHI) specialists and existing EU framework, which help to consider the objective reality of UDPs operating against consumers and subjective perceptions of European society on such UDPs.

However, before exploring the details of the new categorization, this thesis intends to answer one of the most important questions – why to create a new taxonomy? As of the time of writing the thesis, there have already been more than a dozen ways how to categorize UDPs, with of most of them either (i) using new criteria to distinguish practices or (ii) elaborating existing taxonomies with new examples or categories. In this respect, Section 3.1 explains why existing taxonomies would not serve the regulatory objectives described in Chapter II and the reasons for “threat flag” criterion to be appropriate alternative.

3.1. Necessity, clarity, and efficiency of “threat flag” criterion among other taxonomies

In order to prove superiority of “threat flag” criterion among other UDP taxonomies, one (3.1.1) should review such taxonomies, find their deficiencies, and (3.1.2) afterwards explain how the proposal cures them.

3.1.1. Overview of existing taxonomies and their deficiencies

Firstly, one should look at taxonomies of governmental/international organizations, as they are the most related to the enforcement against UDPs. The below chart presents the

summary of taxonomies from EC, EDPB and FTC with criteria used to divide the patterns and other important information related to practical usage of the taxonomies.

Chart 4. Overview of UDPs taxonomies proposed by reputable governmental/international organizations

Author(s) of taxonomy	**Division criteria for categories of dark patterns**	**Important notes from agencies**
European Commission et al., 2022 (Lupianez-Villanueva et al.)	2 criteria, which create 6 categories depending on answers: 1. Choice architecture (how is choice affected): a. Attribute complexity (hides information, which helps to evaluate product/service): high demand message, hidden information, fake reviews, etc. b. Cost complexity (hides information, which helps to understand the price): bait and switch, drip pricing, price comparison prevention, etc. c. Choice complexity (forces to take certain action or make another action more difficult to take): preselection, roach motel, confirm-shaming, etc. 2. Decision-making process (which aspect of consumer behavior is targeted) a. Budget constraint (increases time, costs, effort, attention to take decision): fake reviews, hidden charges, roach motel, etc. b. Shape preferences (persuades on quality / manipulates with consumer needs or ranking of options): confirmshaming, high demand message, bait and switch	1.Taxonomy can be helpful in further analysis the severity of each UDP.[64] 2.The taxonomy should cover not yet existing practices.[65] 3. The taxonomy should cover certain practices, which are recognized as UDPs in certain circumstances, such as infinite scroll, autoplay, unnecessary interruptions, loot boxes and personalization practices.[66]
European Data Protection Board, 2022	6 big categories mostly based on choice architecture varieties, which are further divided into 16 sub-categories: 1. Overloading (presents too many information / options / requests): a. Continuous prompting b. Privacy Maze (difficult to find information because of too many settings / pages). c. Too many options 2. Skipping (misdirects user from reviewing information): a. Deceptive snugness (aka preselection); b. Look over there (aka misdirection); 3. Stirring (appeals to user emotions): a. Emotional steering (for instance, confirm-shaming);	1.Taxonomy promotes GDPR compliance through presentation of non-compliant practices and best practice alternatives.[67] 2.The taxonomy first of all covers UDPs targeted against data privacy rights in social media platforms.[68]

[64] EC Behavioral Study, supra note 7 - p. 38.

[65] *Ibid.* – p. 37.

[66] *Ibid.* – pp. 37-38.

[67] EDPB Guidelines 03/2022, supra note 27 - p. 8.

[68] *Ibid.*

	b. Hidden in plain sight (making information less readable / noticeable) 4. Obstructing (makes certain actions more difficult or impossible to take): a. Dead end (users end up with not working / unavailable function after long search) b. Longer than necessary (too long journey for pro-consumer choice as opposed to pro-business choice); c. Misleading action (discrepancy between presented information and final result) 5. Fickle (makes interface inconsistent and unclear): a. Lacking hierarchy (inconsistency in rankings with information) b. Decontextualising (presenting information in "out of context" place) c. Inconsistent interface 6. Left in the dark (hides information or makes it unclear): a. Conflicting information b. Ambiguous wording or information	3.Their list of "deceptive design patterns" is not exhaustive.[69]
US Federal Trade Commission, 2022	8 categories based on way content of information, the way it is presented and the function which it makes on consumer: 1. Endorsements: fake reviews, false activity, deceptive celebrity endorsement, parasocial relationship pressure; 2. Scarcity: false low stock, false high demand; 3. Urgency: false limited time, false discount, baseless countdown timer; 4. Obstruction: price comparison prevention, roadblocks to cancellation, immortal accounts; 5. Sneaking/hiding information: sneak into basket, hidden information, hidden costs, drip pricing, intermediate currency, forced continuity. 6. Interface interference: misdirection, false hierarchy, disguided ads, bait and switch. 7. Coerced action: unauthorized transactions, auto-play, nagging, forced enrolment, grinding, friend spam; 8. Asymmetric choice: trick questions, confirmshaming, preselection, subverting privacy preferences.	1.Taxonomy promotes e-commerce compliance through presentation of illegal practices, which are and will be targeted by FTC.[70] 2.FTC impliedly states that provided examples are illegal not in all circumstances.[71] 3.The chart in Appendix mentions only "common" dark patterns.[72]

As can be seen from the chart, the above taxonomies try to distinguish UDPs based on the way information or choice is presented to the user, its content and the function of each UDP against the consumer. Nevertheless, this criterion does not allow to clearly delineate categories of UDPs as some of the practices from different categories still look rather similar and/or often exist near each other on webpages *(the relevant practices were highlighted in one color within*

[69] *Ibid.* – p. 3.

[70] Federal Trade Commission, Staff Report "Bringing Dark Patterns to Light" (FTC 2022) – p. 1.

[71] *Ibid.* – p. 20.

[72] *Ibid.* – p. 21.

one chart cell). Moreover, EC and EDPB taxonomies are mostly sector-oriented (on unfair commercial practices and breaches of privacy rights respectively), but "unfair design practices" do not work separately in two fields and often interplay with each other.

Furthermore, only EC taxonomy is intended, according to the authors, to be used further to assess the severity of UDPs, but EC does not explain how it would be done in practice. Overall, the governmental taxonomies cannot be used instead of "threat flag", as they do not resolve the ambiguous interplay of existing acts and serve a mostly informational purpose.

As regards categorizations from non-lawyers, most of them (for instance, *Gray et al.*) help to raise awareness about UDPs and not to regulate fines against these practices.[73] Part of them (for instance, *Bösch et al.*) also focuses on certain online industries only and, thus, cannot be used as tool for comprehensive regulation of UDPs.[74] Still, there are some taxonomies where authors intended to assess the severity of design patterns.

Chart 5. Overview of UDPs taxonomies proposed by professors with intention to differentiate "harmfulness" of UDPs

Author(s) of taxonomy	Division criteria for categories of dark patterns	Important notes from author(s)
Cara, 2019[75]	3 criteria to describe 22 common dark patterns, and one of these criteria is "harmfulness": • Just annoying: confirmshaming, false urgency, infinite scroll, false notifications; • Moderately bad: trick questions, hidden costs, hard opt-out, misdirection; • Very serious: sneak into basket, price comparison prevention, forced continuity, friend spam.	1.The method of article is systematic review of most relevant digital articles, while the purpose of article is just broaden understanding of UDPs.[76]

[73] Gray et al., 'The dark (patterns) side of UX design' [2018], Proceedings of the 2018 CHI conference on human factors in computing systems, 1-14.

[74] Bösch et al., 'Tales from the Dark Side: Privacy Dark Strategies and Privacy Dark Patterns' [2016], Proceedings on Privacy Enhancing Technologies, 237-254.

[75] Cara Corina, Dark Patterns In The Media: A Systematic Review [2019], Network Intelligence Studies, Vol. VII (14), 106-113.

[76] *Ibid.* – p. 106.

		2.The author admits it is difficult to regulate them because of "fine line" between UDPs and a honest user experience enhancing elements".[77]
Mathur et al, 2021[78]	6 features of UDPs based on choice architecture and information flow, combination of which may be present in various patterns: • Asymmetric (unequal burdens on available choices); • Restrictive (elimination of important choices); • Disparate Treatment; • Covert (indirectly leading to certain choices); • Deceptive; • Information Hiding. Also, they presented 4 "normative lenses", evaluation of which may help to assess the harmfulness of UDPs: • Individual welfare; • Collective welfare; • Regulatory objectives; • Individual autonomy.	1.The authors admit that each of "normative lenses" present different ways how to evaluate UDPs.[79] 2.There can be relative or absolute threshold to determine whether some practice constitute UDP, but this requires careful normative justification.[80]
Lesser and Yang, 2022[81]	"Four-level hierarchical taxonomy" based on the "influence" instrument against users: 1. Information Asymmetry: a. Active Misleading Actions: i. Misleading Information: fake urgency or endorsements; ii. Misleading Presentation: trick questions, misdirection, b. Passive Misleading Omissions: i. Hiding Information: price comparison prevention; ii. Delaying Provision: hidden costs; 2. Free Choice Repression: a. Undesirable Imposition: i. Pressure Imposing: pressured selling; ii. Forced Acceptance: sneak into basket, bait and switch; b. Undesirable Restriction: i. Restricting Specific Users: Pay to Skip.	1.The proposed taxonomy will be consistent with UCPD structure (*Information Asymmetry covers misleading practices, while Free Choice Repression – aggressive and other unfair practices*).[82] 2.However, the authors admit UCPD will not always apply to some of categories.[83] 3.The authors also agree on lack of clarity in UCPD regulation against UDPs, so propose

[77] *Ibid.* – p. 108.

[78] Mathur et al., 2021, supra note 24.

[79] *Ibid.* – p. 19.

[80] *Ibid.* – p. 23.

[81] Leiser Mark and Yang Wen-Ting, Illuminating manipulative design: From 'dark patterns' to information asymmetry and the repression of free choice under the Unfair Commercial Practices Directive [2022].

[82] *Ibid.* – pp. 1 and 18.

[83] *Ibid.* – p. 21.

	ii. Restricting Specific Actions: roach motel.	adoption of "Codes for Dark Patterns".[84]

Nevertheless, each of these taxonomies has certain deficiencies in achieving regulatory objectives from Chapter II. In the first taxonomy, the author proposes her own view on the level of threat from each practice, but does not explain how such level was assessed and whether it would serve as objective criteria for legal purposes. The remaining taxonomies only present the criteria to assess "harmfulness" of UDPs, but both admit the lack of clarity on how to apply these criteria in practice. In their earlier work, *Mathur et al.* mentioned that some UDPs existed in "gray area",[85] while *Lesser and Yang* agreed that UCPD would not apply to some of UDPs mentioned in their work.[86]

3.1.2. Advantages of proposed criterion in improving current EU regulation of UDPs

In response to problems of existing taxonomies for regulation purposes, this thesis introduces a new "threat flag" criterion. There is no intention to repeal existing developments or describe them as inappropriate. Instead, we will take into account different features of these developments and tailor them to regulatory objectives from Chapter II.

Firstly, "threat flag" criterion is not based primarily on choice architecture and the function which each UDP performs. As shown on charts above, there will always be contention points on where to place certain UDP. However, the key idea here is to establish the level of threat in comparison to other designs instead of continuously looking for similarities between UDPs, unless this is really necessary in assessing the mentioned level of threat. Similarly, there is not much focus on the type of EU acts, which govern specific UDPs, because the criterion

[84] *Ibid.* – pp. 28-29.

[85] Mathur et al., 2019, supra note 25 - p. 81.26.

[86] Leiser and Yang, supra note 81 - p. 21.

proposes a unified regulatory approach to all UDPs instead of trying to find the ambiguous line between practices governed by UCPD, GDPR, DSA or other acts.

Secondly, new criterion would partially serve as prohibitory provision as alternative to a number of "information requirements" from existing EU acts, which unfortunately does not work effectively in tackling the problem.

Finally, the new criterion would help to achieve "effective, proportionate, and dissuasive" penalties against unfair design practices. As opposed to old taxonomies, the criterion considers existing case studies and surveys on effectiveness of certain practices against consumers and different harms as results of such practices. The assigned "flags" to UDPs will serve as a good starting point for national consumer or data protection agencies to establish the fine, which would properly reflect the danger of certain UDP and be predictable for all stakeholders.

3.2. Detailed exploration of criteria for the new UDPs taxonomy

The idea of the new taxonomy is to assess the threat of each UDP with the help of the "distortion" and "harm" criteria. The next Section includes the attempts to assess both factors only with respect to the most popular dark patterns. Nevertheless, the success and harm of "unfair design pattern" against consumer cannot precisely evaluated in advance and may be different, taking into account the use of several dark patterns simultaneously or the circumstances of particular consumers.

Hence, the thesis proposes results to establish certain presumptions on each UDP's effect on "average consumer" in line with EU law, with each of stakeholders being able to challenge these preliminary evaluations in each case. Such approach helps to achieve a balance between

predictability of consequences for all stakeholders and proportionality of such consequences for each individual case.

3.2.1. Distortion criterion: differentiating unfair and simply persuasive practices

First and foremost, what does "distortion" mean with respect to unfair design practices? According to the UCPD, the distortion of consumers' economic behavior makes or is likely to make such consumers take transactional decision (purchasing product, visiting website, staying more with the service) that they would not have taken otherwise.[87] Hence, we need to review the capability of common UDPs to make consumers make unwanted decisions online and compare such effectiveness.

Before proceeding to comparison of UDPs' capability of distortion, one should briefly mention the most popular practices. In *2022 EC Behavioral Study*, the EC mentioned top-10 practices (hidden information / false hierarchy, preselection, nagging, hard to cancel, forced registration, disguised ad, time-limited message, toying with emotion, hidden costs, and intermediate currency),[88] while OECD also referred to urgency-related and social proof-related practices.[89]

There is no comprehensive case study which compared each and every UDP. Instead, most of the studies compare only several UDPs, choosing either by popularity,[90] similarity

[87] UCPD Commission Guidance, supra note 9 – Section 2.4.

[88] EC Behavioral Study, supra note 7 – Figure 2.

[89] OECD, 'Dark commercial patterns' [2022] OECD Digital Economy Papers, No. 336, OECD Publishing – p. 5.

[90] Di Geronimo et al., 'UI Dark Patterns and Where to Find Them: A Study on Mobile Applications and User Perception' [2020] , CHI Conference on Human Factors in Computing Systems 1-14; Luguri Jamie and Strahilevitz Lior, Shining a Light on Dark Patterns [2021], 13 Journal of Legal Analysis 43; Bongard-Blanchy et al., Dark Patterns from the End-User Perspective [2021], ACM DIS Conference on Designing interactive systems.

(pricing practices, scarcity cues, etc.),[91] or the platform or place in interface, where such practice are used (desktop vs mobile, during registration, for consent banners or during presentation of price, etc.).[92] Indeed, there is a point among some specialists that detectability of UDP has "a slight inverse correlation" with the likelihood of influencing consumers.[93] However, one shall use it just as secondary factor in assessment, as there are many cases of UDPs, which can be effective despite their detectability. For instance, roach motel (hard to cancel) or other severe cases of obstruction strategies can be easily detectable by consumers once they want to cancel or change something, but that does not change the fact of consumer being unable to do so. The cases of limited quantity or time can also be understood by consumers as being probably untruthful, yet they may still choose the not so desired option because of having a slight fear that the message can actually be true.

In this respect, this assessment of "distortion" of most common UDPs takes various factors of each UDP earlier tested in case studies, tries to find certain tendencies and apply them by analogy to those practices not assessed earlier. Still, such case studies can be done by governmental agencies or EU bodies in the future in order to make slight changes to this assessment.

First of all, one should look at the most "successful" practices according to case studies. For instance, several authors recognize "hidden information" as one of the most effective

[91] Santana et al., Consumer Reactions to Drip Pricing [2010], Marketing Science 39(1), 188-210; Jeong Hyun Ju and Kwon Kyoung-Nan, The Effectiveness of Two Online Persuasion Claims: Limited Product Availability and Product Popularity [2012], Journal of Promotion Management 18:1, 83-99.

[92] Graßl et al, Dark and bright patterns in cookie consent requests [2020], Journal of Digital Social Research 3(2); Utz, C., Degeling, M., Fahl, S., Schaub, F., Holz, T. 2019. (Un)informed consent: studying GDPR consent notices in the field. In Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security, 973-990; Ahmetoglu et al, Pricing practices: A critical review of their effects on consumer perceptions and behaviour [2014], Journal of Retailing and Consumer Services 21(5), 696-707.

[93] Bongard-Blanchy et al., supra note 90 - page 770.

UDPs,[94] while *Luguri & Strahivelitz* also mention "trick questions" and different obstruction strategies as being slightly less effective than hiding information (23,6 percentage points for hard to cancel and 20,1 percentage points for preselection against 30,1 percentage points for hidden information in case study).[95] Besides this, the EC recognized that forced action (especially if combined with personalization) can strongly affect the consumers' behavior.[96]

The reason for "success" for hidden information may be the fact that dishonest businesses tend to hide some important information, so that the likelihood of having difference in perception of product or service in presence or absence of such practice is higher than for other online practices. Accordingly, any unfair design practice which concerns hiding important information in different way (hidden costs, hidden subscription, sneak into basket when it is not properly disclosed) shall be presumed to cause the same level of distortion for consumers. As regards obstruction strategies, there may be several reasons for their effectiveness, for instance, (i) lesser proficiency of some people groups in handling non-user-friendly interface and (ii) online fatigue of consumers, who spent much time on long questionnaires, registration or ordering process and simply want to conclude the process as soon as possible without making additional actions. With respect to forced actions, their effectiveness is often based on value of product or service given in return, so that consumer is forced to perform some not strictly necessary things to receive something they really want.

Secondly, there are certain practices in relation to which there is no consensus on their high level of distortion. For instance, *Jeong & Know* found social proof (and confirm-shaming

[94] EC Behavioral Study, supra note 7 – p. 7; OECD, supra note 89 – p. 5, Luguri and Strahivelitz, supra note 90 - p. 47.

[95] Luguri and Strahivelitz, supra note 90 - p. 75.

[96] EC Behavioral Study, supra note 7 - p. 95

for *Luguri and Strahivelitz)* could be almost as effective as some obstruction strategies, whereas scarcity was less effective against consumers.[97] At the same time, *Sin et al.* stated that social proof and scarcity could be similarly effective,[98] while the EC considered confirm-shaming to be ineffective against EU consumers.[99] Furthermore, Santana et al. made case study showing that drip pricing caused 24,5% consumers (which is rather high) to make financial mistake in comparing similar options and choosing the cheaper one.[100] However, *Huck &Wallace* found that drip pricing is less effective than time-limited offers (similar to scarcity), while baiting and reference pricing (for instance, fake discount) have even less influence.[101]

Thirdly, considering the lack of consensus on certain practices, one should understand the difference in circumstances of case studies, including without limitation the place of interface where the practice was used or the type of product being offered. For example, the EC considered "toying with emotions" (with confirm-shaming being one example) only half as effective as hidden information, but personalization techniques increased such effectiveness approximately by a half because of data-driven practices being more targeted against particular consumers.[102] Also, obstruction strategies work particularly well in cookie consent banners,[103] whereas baiting can be actually effective in relation to physical products because of approximately 62% customers substituting the stock-out in the same store instead of going

[97] Luguri and Strahivelitz, supra note 90 - p. 75; Jeong and Kwon, supra note 91 – pp. 94-95.

[98] Sin et al, supra note 2 - p. 8.

[99] EC Behavioral Study, supra note 7 – p. 88-89.

[100] Santana et al., supra note 91 - p. 196.

[101] Huck Steffen and Wallace Brian, The impact of price frames on consumer decision making: Experimental evidence [2015] – p. 2.

[102] EC Behavioral Study, supra note 7 - pp. 40, 105-106.

[103] Machuletz Dominique and Böhme Rainer, Multiple Purposes, Multiple Problems: A User Study of Consent Dialogs after GDPR [2019], Proceedings on Privacy Enhancing Technologies, 2020(2), 481-498 – pp. 493-494; Utz et al., supra note 92 – pp. 985-986.

somewhere else.[104] The limited time message almost had no influence first of all on "free trial" offers.[105]

Therefore, in consideration of above case studies, it is proposed to categorize most common UDPs in the following way:

Chart 6. Categorization of UDPs depending on their capability to cause "distortion" for consumers' behavior

Low	Middle	High	Severe
1.Baiting, bait and switch (for online products); 2.Reference pricing, complex pricing; 3.Social proof- and urgency-related claims (for money-free services or free trials)	1.Baiting, bait and switch (for physical products); 2.Toying with emotions (not personalized, includes confirmshaming); 3.Social proof- and urgency-related claims; 4.Drip pricing.	1.Ambigious information (trick questions, price comparison prevention, conflicting information, lacking hierarchy) 2.Obstruction strategies (preselection, hard to cancel, longer than necessary, inconsistent interface); 3.Toying with emotions (personalized, data-driven); 4.Forced actions (including forced registration, forced continuity, continuous prompting).	1.Hidden information, hidden costs, hidden subscription; 2.Sneak into basket (when hiding information); 3.Obstruction strategies in cookie banners and other privacy options (preselection, hard to cancel, immortal accounts, longer than necessary, Privacy Maze).

Several important considerations should be mentioned in order to properly understand this chart. Some of the abovementioned practices were not covered in case studies, but this thesis proposes to apply categorization to them based on analogy due to certain similarities with earlier assessed practices. Besides this, the fact that some practices are placed in "green" zone does not *per se* mean that they should always be considered legal. As explained in Sections 3.2.2 and 3.3, we also need to assess the harm of such practices to "average

[104] Zinn Walter and Liu Peter, Consumer Response to Retail Stockouts [2001], Journal of Business Logistics 22(1), 49-71. – p. 59.

[105] Luguri and Strahilevitz, supra note 90 - p. 76.

consumer", so that certain practices with low "distortion" rate should be recognized as more dangerous to EU consumers than other simply persuasive, yet not harmful practices. Finally, this thesis only sets the preliminary idea on how to categorize UDPs to achieve regulatory objectives from Chapter II. The regulatory authorities and HCI specialists are indeed encouraged to correct the presented view here and further update the "level of threat" of each UDP from time to time based on new developments in e-commerce.

3.2.2. Harm criterion: the EU values in the need of proportionate protection

There are various ways how unfair design practices can harm end users. As mentioned in Section 3.1.1, *Mathur et al.* proposed to analyze UDPs through 4 several normative lenses, one of which concerns individual welfare. In the view of authors, this welfare is being often attacked by unfair design practices and, as a result, lead to 1)financial losses because of consumers spending more than initially intended; 2)privacy harms caused by oversharing the personal data or losing control over its processing, etc.; and 3)cognitive burdens wasting users' time and energy.[106] While the *OECD* similarly describes key categories of harm caused by UDPs (except for third category, where negative emotions and risk of addiction to the digital services fit in),[107] *Godel et al.* propose to categorize digital consumers harms based on both outcome and processes leading to certain outcome.[108] Under this methodology, the authors divide the harms as a result of 1)barriers to personal autonomy in overall; 2)provision of misleading information; 3)barriers to switching the services in particular; 4)unfair processing of personal data; and 5)being overcharged for services, either with money or shared personal

[106] Mathur et al, 2021, supra note 24 - pp. 14-15.

[107] OECD, supra note 89 – pp. 24-25.

[108] Godel et al., Digital consumer harms - A taxonomy, root cause analysis and methodologies for measurement (London Economics 2023) – p. 9.

data.[109] This all proves that consumers can be harmed differently by UDPs, and much of these harms are not of purely monetary nature.

So, how should one assess these harms and compare with other ones in order to create "harm" criterion for UDPs? For instance, the UK Information Commissioner's Office notes problems in the processing of personal data can cause both countable financial losses and hardly countable psychological detriment, but (i) the privacy harms are often based on probabilities (data subject may not be aware of breach or data breach occurred, but no one used data against user), (ii) some data may be valuable only in aggregate form, but not about individual person, and (iii) users value their privacy differently.[110]

On the first point, there is CJEU's position that not every infringement of GDPR gives victims the right of compensation because not all infringements lead to damages.[111] As regards users' perception on privacy, there is an interesting survey made by *Winegar and Sunstein* showing that consumers are willing to pay only USD 5 / month on average to delete all of their personal data collected by businesses, while the companies are ready to pay USD 80 / month per consumer to receive full access to such data.[112] While the survey concerned US citizens, it is believed that results could be rather similar in the European Union, meaning that consumers usually does not perceive their personal data to be valuable. To the contrary, overview of EU Charter of Fundamental Rights, European Convention of Human Rights as well as comparison

[109] *Ibid.*

[110] Information Commissioner's Office, Overview of Data Protection Harms and the ICO's Taxonomy (Information Commissioner's Office 2022) – pp. 3-6.

[111] Case C-300/21 *UI v Österreichische Post AG* [2023] OJ C195/02.

[112] Winegar, Angela G. and Sunstein, Cass R., How Much Is Data Privacy Worth? A Preliminary Investigation [2019], Journal of Consumer Policy - p. 3.

of administrative fines enshrined in GDPR and consumer protection directives[113] creates an impression that privacy rights are much more important to individuals and the society in general.

Considering the above and the fact that this thesis wants to define "threat flags" of UDPs *in abstracto* (since most EU acts already have such criteria, as duration, number of victims, losses of consumers), it is proposed not to decide whether privacy harms are more or less severe than financial losses. Instead, both types of harms to "average consumer" are divided into 4 groups (just as it was in Section 3.1.2 above) taking into account the issues of data protection for individual and society, market economy, problems of overconsumption,

Chart 6. Assessment of level of harms caused to consumers depending on UDPs' outcome

Low	Middle	High	Severe
1.Loss of time due to using service / product longer (to stay on website or in app longer)	1.Unlawful processing of non-sensitive data for aggregate information (analytics)	1.Unlawful processing of non-sensitive data for marketing and targeted advertising	1.Unlawful processing of (i) sensitive data or (ii) data for decisions with legal effect:
2. Loss of time due to becoming interested in free service / product (visiting website, installing product)	2. Financial losses due to impulse buying	2. Financial losses due to misleading purchase	2. Financial losses due to authorized charges

The reasons to include each harm in respective column are the following. Firstly, "the loss of time" harm was placed in the "green" zone because in such case the consumers do not involuntarily share their personal data or pay for something undesired, so two key categories of digital consumer harm are not triggered.

[113] Charter of Fundamental Rights of the European Union [2012] OJ C326/26 - Articles 7-8, 17, and 38; Council of Europe, European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14 [1950], ETS 5 – Article 8, Article 1 of Protocol No. 1, GDPR, supra note 39 – Article 83, UCPD, supra note 28 – Article 13.

Secondly, the unlawful processing data in aggregate form is placed in "middle harm" zone, since the data of individual "average consumer" in this case is less valuable to both consumer and business as opposed to sensitive data or data necessary to target individual. As regards impulse buying, it definitely causes overconsumption, which is not beneficial for one end users, but to certain extent fuels the economy of so many honest businesses.

Thirdly, misleading purchases are definitely worse than impulse buying, as the buyer receives something not expected. As regards data for marketing and targeted advertising, it is more valuable to society, and its unlawful usage directly impacts the consumer, including through personalization techniques.

Fourthly, unlawful usage of sensitive data and data for the purposes of decision-making with legal effects are prohibited with the highest fines in the GDPR, so that privacy harm caused by such usage should be placed in "red" zone. The authorized charges are worse than misleading purchases, as the consumer here pays for nothing or something not even wanted or at all.

Hence, it is believed that the above chart of digital consumer harms is a proper way to further assess the harm caused by each type of UDPs. Considering the most common harm attributed to each type of UDP, this chart allows to establish separate categorization of UDPs as criteria in the proposed "threat flag" taxonomy.

Chart 7. Categorization of UDPs depending on their "harm" to "average consumer"

Low	Middle	High	Severe
1.UDPs commonly related to using the service longer: • Toying with emotions (not	1.UDPs commonly related to share of data for analytics: • Obstruction strategies in cookie banners (preselection, hard to cancel, false hierarchy).	1.UDPs commonly related to share of data for marketing and targeted advertising: • Preselection; • Continuous prompting;	1.UDPs commonly related to sharing of sensitive data or data for decisions with legal effect: • Toying with emotions (personalized)

personalized); • Longer than necessary • False hierarchy		• Inconsistent interface; • Trick questions; • Toying with emotions (not personalized)	• Immortal accounts; • Forced registration
2.UDPs commonly related to becoming interested in free service: • Baiting, bait and switch.	2.UDP commonly related to impulse buying: • Baiting, bait and switch • False hierarchy • Reference pricing, complex pricing • Price comparison prevention • Toying with emotions (not personalized) • Urgency-related claims	2.UDP commonly related to misleading purchases: • Hidden information • Conflicting information • Social proof-related claims	2.UDPs commonly related to unauthorized charges: • Preselection; • Forced continuity; • Hidden costs, hidden subscription, sneak into basket • Hard to cancel • Drip pricing.

As can be seen from the above chart, most of the UDPs can be attributed to a particular type of common digital consumer harm. Although some UDPs still work rather differently, it is still possible to define their "threat flag" in Section 3.3 depending on the place in interface where such practice is used.

3.3. Incorporation of criteria into new "threat flag" taxonomy of UDPs

Once there is an understanding of how most common UDPs affect the consumers and which effectiveness they have against them, it is possible to assign "threat flag" to them. This thesis proposes to establish "threat flag" based on (i) average value of "distortion" and "harm" criteria with (ii) prevailing effect of the latter one in case of having average value between two zones. Accordingly, using the result of assessment from previous Sections, one can assign the following "threat flag" to most common "unfair design practices".

Chart 8. Assessment of "threat flag" of each UDP depending on the level of "harm" and "distortion"

Severe		Drip pricing	Obstruction strategies for payments (preselection, hard to cancel, Personalized toying with emotions Forced registration, forced continuity	Hidden costs, hidden subscription, sneak into basket Immortal accounts
High	Social proof-related claims (for free services / products or trials)	Social proof-related claims (for paid services / products) Not personalized toying with emotions (when related to sharing of data)	Ambiguous information (trick questions, conflicting information, inconsistent interface) Continuous prompting	Preselection (for other privacy options), Privacy Maze Hidden information
Middle	Baiting, bait and switch (for paid online services / products) Urgency-related claims (for free services / products or trials) Reference pricing, complex pricing	Baiting, bait and switch (for paid physical products) Not personalized toying with emotions (when related to payment) Urgency-related claims (for paid services / products)	Price comparison prevention False hierarchy (for payments)	Obstruction strategies in cookie-banners (preselection, hard to cancel, false hierarchy) Longer than necessary (for cookie banners and other privacy options)
Low	Baiting, bait and switch (for free online products)	Not personalized toying with emotions (for free products; when not related to payment or sharing of data)	False hierarchy, Longer than necessary (for free products; when not related to payment or sharing of data)	
Harm **Distortion**	**Low**	**Middle**	**High**	**Superhigh**

The reason why this approach for categorization is used is twofold. Firstly, both criteria have similarly important to understand the overall harm caused to "average consumer", as one criterion assesses the individual harm caused to such consumer and the second one defines the likelihood of such harm. Secondly, at the same time, the case studies from Section 3.2.1 show that the difference in range in percentages of people affected by most common UDPs is not so serious, contrary to the possibilities of harm caused by them. This means that one should consider "harm" criterion as having more value in assessment and give it priority.

Once the "threat flag" of each UDP is established, there are important questions (i) how to use this categorization in practice and (ii) what the ways of are incorporating the taxonomy into current EU legal architecture of regulating "unfair design practices". Firstly, "threat flag" helps to understand the illegality of the practice and, hence, practices within "green" zone should be presumed to be legal and legitimate in e-commerce, while other zones represent different levels of illegality (from yellow as slightly not compliant to red as seriously non-compliant). Based on such differentiation, the regulatory authorities can define the ranges of penalties that apply in relation to each zone of "threat flag (for instance, 0-25% of maximum administrative fines for yellow zone, 25-50% for orange zone, and 50-100% for red zone). Should certain e-commerce apply several UDPs on its website or app, the DPA or consumer protection agency may separately calculate penalties to each UDP and afterwards establish the total fine for the business.

However, the categorization presented in this thesis should serve only as a starting point in calculation of fines and assist other existing criteria in EU acts, discussed earlier in Section 2.3. All stakeholders are also free to challenge the presumption of "threat flag" established for particular UDPs, yet they will carry the burden of proof in this case.

Secondly, there is contentious point how to properly incorporate the proposed categorization into existing current EU acts. The most revolutionary approach would be to create separate regulation on "unfair design practices" (which was also proposed by *Leiser and Yang*),[114] yet it would take much time and resources for EU bodies to properly harmonize this rather wide sphere and mention as many UDPs in the chart as possible. Also, since for long time the countries have their own local laws which simply transposed consumer protection directive, the proposal for new wide consumer protection regulation would highly likely be

[114] Leiser and Yang, supra note 81 - p. 29.

greeted with serious opposition from most of EU Member States. As alternative to regulation, the EU can adopt separate directive on UDPs, which would allow the states to transpose the ideas proposed in the thesis in convenient way for them. Nevertheless, this does not solve the problem that EU bodies would spend enormous time and resources to agree on categorization of each UDP so as to avoid making many changes to the chart in the future (as the process for changes is not expedient).

Hence, in my opinion, the best way how the chart can be incorporated into the current EU system is to adopt separate guidelines together by the EC in consultation with EDPB, local DPA, consumer protection agencies, and digital services coordinators, which shall be used by the regulatory authorities during the calculation of fines under existing EU acts related to "unfair design practices". This would give flexibility for the EU bodies to quickly bring the changes to the chart (if certain studies or other evidence gives new information on effectiveness of certain UDPs), while having the required predictability of consequences because of obligatory nature of guidelines.

CONCLUSION

Based on this thesis and many other existing works on "unfair design practices", it is evident that the problem of their consistent usage against consumers is serious and, hence, there must be effective EU regulation against them. However, as presented in Chapter II, the current EU system is definitely not ideal, because it consists of fragmentary and simultaneously overlapping regulations and directives related to UDPs, application of which is neither clear nor predictable for consumers and e-commerce businesses. The EU general liability system against UDPs is also not systematic and consistent through EU Member States.

In response to that, this thesis proposed an alternative approach to the regulation of "unfair design practices", which first of all includes repealing "dark patterns" term as less neutral, non-inclusive, and not consistent with the EU law term. The next key proposal is the introduction "threat flag" criterion, based on which each UDP is assessed based on their "harm" to consumers and "distortion" of economic behavior. Such "threat flag" is to be further used in assessing the illegality of certain practice and administrative fines applicable to infringers.

Indeed, the proposed categorization may not be completely correct in relation to all cases and that it is difficult to introduce proposed amendments in the current EU legal system. For these reasons, the categorization serves only as one of the factors of calculation of fines, and either stakeholder may discharge the burden of proving that certain practice is less or more harmful in particular cases than as it was assigned in this thesis. Moreover, the EU Member States are free to decide which ways is the best for them to introduce this change, while the thesis explains several options that can be done to make the regulation better.

BIBLIOGRAPHY

Statutes and bills

Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act).

Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) [2022] OJ 2 265.

Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce') [2000] OJ 2 178.

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) [2002] OJ 2 201.

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ 2 119.

Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the

European Parliament and of the Council (Unfair Commercial Practices Directive) [2005] OJ 2 149.

Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council [2011] OJ 2 304.

Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts [1993] OJ 2 095.

Charter of Fundamental Rights of the European Union [2012] OJ C326/26/

Council of Europe, European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14 [1950], ETS 5.

Governmental guidelines

European Commission, Directorate-General for Justice and Consumers, Lupiáñez-Villanueva et al., 'Behavioural study on unfair commercial practices in the digital environment: dark patterns and manipulative personalisation: final report' [2002], Publications Office of the European Union.

Guidance on the interpretation and application of Directive 2005/29/EC of the European Parliament and of the Council concerning unfair business-to-consumer commercial practices in the internal market [2021] OJ 1 526.

CNIL, 'IP Report: Shaping Choices in the Digital World' [2019] 6 Laboratoire d’Innovation Numerique de la CNIL.

Autoriteit Consument & Markt, 'IP Protection of the online consumer: Boundaries of online persuasion' (Autoriteit Consument & Markt, 2020).

Datatilsynet, 'Digital Services and Consumer Data' (Datatilsynet, 2020).

European Data Protection Board, Guidelines 03/2022 on Deceptive design patterns in social media platform interfaces (European Data Protection Board 2023).

Department for Business, Energy, and Industrial Strategy (BEIS), Reforming Competition and Consumer Policy (2021).

European Data Protection Board, Guidelines 4/2019 on Article 25 Data Protection by Design and by Default (European Data Protection Board 2020).

Guidance on the interpretation and application of Directive 2011/83/EU of the European Parliament and of the Council on consumer rights [2021] OJ 1 525.

Guidance on the interpretation and application of Council Directive 93/13/EEC on unfair terms in consumer contracts [2019] OJ 1 323.

European Data Protection Board, Guidelines 04/2022 on the calculation of administrative fines under the GDPR (European Data Protection Board 2023).

Autoriteit persoonsgegevens, Beleidsregels van de Autoriteit Persoonsgegevens van 19 februari 2019 met betrekking tot het bepalen van de hoogte van bestuurlijke boetes (Boetebeleidsregels Autoriteit Persoonsgegevens 2019) (Staatscourant 2019).

Konferenz der unabhängigen datenschutzaufsichtsbehörden des bundes und der länder, Konzept der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder zur Bußgeldzumessung in Verfahren gegen Unternehmen (Datenschutzkonferenz 2019).

Federal Trade Commission, Staff Report “Bringing Dark Patterns to Light” (FTC 2022).

Information Commissioner's Office, Overview of Data Protection Harms and the ICO’s Taxonomy (Information Commissioner's Office 2022).

Cases and investigations

CNIL Restricted Committee, 'Deliberation of the restricted committee No SAN-2021-024 of 31 December 2021 concerning FACEBOOK IRELAND LIMITED' (*CNIL*, 31 December 2021) <https://www.cnil.fr/sites/default/files/atoms/files/deliberation_of_the_restricted_committee_no._san-2021-024_of_31_december_2021_concerning_facebook_ireland_limited.pdf> accessed 28 May 2023.

Autorite de protection des donnees Gegevensbeschermingsautoriteit, 'Décision quant au fond 103/2022 du 16 juin 2022' (16 June 2022) <https://www.autoriteprotectiondonnees.be/publications/decision-quant-au-fond-n-103-2022.pdf> accessed 28 May 2023.

Garante per za Protezione dei Dati Personali, ' Provvedimento inibitorio, prescrittivo e sanzionatorio nei confronti di Edison Energia S.p.A. - 15 dicembre 2022 [9856345]' (15 December 2022) <https://www.autoriteprotectiondonnees.be/publications/decision-quant-au-fond-n-103-2022.pdf> accessed 28 May 2023.

Gazdasági Versenyhivatal, 'Határozatot a Booking.com ellen' (2018) < https://gvh.hu/pfile/file?path=/dontesek/versenyhivatali_dontesek/versenyhivatali_dontesek/dontesek_2018/vj017_2018_m&inline=true > accessed 28 May 2023

ACM, ' Decision of the Netherlands Authority for Consumers and Markets regarding the imposition of a fine on TRENDX B.V' (2022) < https://www.acm.nl/system/files/documents/decision-fine-trendx.pdf > accessed 28 May 2023.

Case C-300/21 UI v Österreichische Post AG [2023] OJ C195/02.

Books and periodical materials

Ray Sin et al., 'Dark patterns in online shopping: do they work and can nudges help mitigate impulse buying?' [2022] Behavioural Public Policy, Cambridge University Press 1-27.

Maier et al., 'DARK DESIGN PATTERNS: AN END-USER PERSPECTIVE' [2020] 16(2) Human Technology 170-199.

Mathur et al., 'Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites' [2019] 3(CSCW), Article 81, Proceedings of the ACM on Human-Computer Interaction, 1-32.

Di Geronimo et al., 'UI Dark Patterns and Where to Find Them: A Study on Mobile Applications and User Perception' [2020] , CHI Conference on Human Factors in Computing Systems 1-14.

Gunawan et al., 'A Comparative Study of Dark Patterns Across Mobile and Web Modalities' [2021] 5(CSCW2), Article 377, Proceedings of the ACM on Human-Computer Interaction, 1-29.

OECD, 'Dark commercial patterns' [2022] OECD Digital Economy Papers, No. 336, OECD Publishing.

Chugh et al., 'Unpacking dark patterns: understanding dark patterns and their implications for consumer protection in the digital economy' [2021] 7(1), RGNUL Student Research Review.

Mathur et al., 'What Makes a Dark Pattern... Dark? Design Attributes, Normative Considerations, and Measurement Methods ' [2021] Proceedings of the CHI Conference on Human Factors in Computing Systems, 1-18.

BEUC, "DARK PATTERNS" AND THE EU CONSUMER LAW ACQUIS (BEUC 2022).

Tobias Nyström and Agnis Stibe, When Persuasive Technology Gets Dark?. in Themistocleous and others (eds), Information Systems: 17th European, Mediterranean, and Middle Eastern Conference (Springer 2020).

Gray et al., 'The dark (patterns) side of UX design' [2018], Proceedings of the 2018 CHI conference on human factors in computing systems, 1-14.

Bösch et al., 'Tales from the Dark Side: Privacy Dark Strategies and Privacy Dark Patterns' [2016], Proceedings on Privacy Enhancing Technologies, 237-254.

Cara Corina, Dark Patterns In The Media: A Systematic Review [2019], Network Intelligence Studies, Vol. VII (14), 106-113.

Leiser Mark and Yang Wen-Ting, Illuminating manipulative design: From 'dark patterns' to information asymmetry and the repression of free choice under the Unfair Commercial Practices Directive [2022].

Luguri Jamie and Strahilevitz Lior, Shining a Light on Dark Patterns [2021], 13 Journal of Legal Analysis 43.

Bongard-Blanchy et al., Dark Patterns from the End-User Perspective [2021], ACM DIS Conference on Designing interactive systems.

Santana et al., Consumer Reactions to Drip Pricing [2010], Marketing Science 39(1), 188-210.

Jeong Hyun Ju and Kwon Kyoung-Nan, The Effectiveness of Two Online Persuasion Claims: Limited Product Availability and Product Popularity [2012], Journal of Promotion Management 18:1, 83-99.

Graßl et al, Dark and bright patterns in cookie consent requests [2020], Journal of Digital Social Research 3(2).

Utz, C., Degeling, M., Fahl, S., Schaub, F., Holz, T. 2019. (Un)informed consent: studying GDPR consent notices in the field. In Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security, 973-990.

Ahmetoglu et al, Pricing practices: A critical review of their effects on consumer perceptions and behaviour [2014], Journal of Retailing and Consumer Services 21(5), 696-707.

Huck Steffen and Wallace Brian, The impact of price frames on consumer decision making: Experimental evidence [2015].

Machuletz Dominique and Böhme Rainer, Multiple Purposes, Multiple Problems: A User Study of Consent Dialogs after GDPR [2019], Proceedings on Privacy Enhancing Technologies, 2020(2), 481-498.

Zinn Walter and Liu Peter, Consumer Response to Retail Stockouts [2001], Journal of Business Logistics 22(1), 49-71.

Godel et al., Digital consumer harms - A taxonomy, root cause analysis and methodologies for measurement (London Economics 2023).

Winegar, Angela G. and Sunstein, Cass R., How Much Is Data Privacy Worth? A Preliminary Investigation [2019], Journal of Consumer Policy.

Internet resources

Eurostat, 'E-commerce continues to grow in the EU' (*Eurostat*, 28 February 2023) <https://ec.europa.eu/eurostat/web/products-eurostat-news/w/DDN-20230228-2> accessed 5 April 2023.

Harry Brignull, 'Bringing Dark Patterns to Light' (*Medium*, 6 June 2021) <https://harrybr.medium.com/bringing-dark-patterns-to-light-d86f24224ebf> accessed 5 April 2023.

Alex Hill, 'The real impact of dark UX patterns' (*UX Collective, Medium*, 13 January 2022) <https://uxdesign.cc/the-real-impact-of-dark-ux-patterns-fade9d1ca2c6> accessed 5 April 2023.

Zipboard, 'Dark Patterns Harm Usability' (*ZipBoard, Medium*, 21 November 2017) <https://blog.zipboard.co/dark-patterns-harm-usability-5b75e293e7a7> accessed 5 April 2023.

European commission, 'Consumer protection: manipulative online practices found on 148 out of 399 online shops screened' (*European Commission*, 30 January 2023) <https://ec.europa.eu/commission/presscorner/detail/en/ip_23_418> accessed 5 April 2023.

Privacy108, 'EU's New Deal for Consumers: a dark future for dark patterns' (*Privacy108*, 24 June 2022) <https://privacy108.com.au/insights/eus-new-deal-for-consumers/> accessed 5 April 2023.

Ecommerce Europe, 'Commission publishes updated guidance documents on the Omnibus Directive' (*ECommerce Europe*, 7 January 2022) <https://ecommerce-europe.eu/news-item/commission-publishes-updated-guidance-documents-on-the-omnibus-directive/> accessed 5 April 2023.

Portfolio, 'Hungary slaps record fine of EUR 7 million on Booking.com' (*Portfolio*, 20 May 2020) <https://www.portfolio.hu/en/business/20200520/hungary-slaps-record-fine-of-eur-7-million-on-bookingcom-432994> accessed 5 April 2023.

BBC, 'France fines Google and Facebook over cookies' (*BBC*, 7 January 2022) <https://www.bbc.com/news/technology-59909647> accessed 5 April 2023.

Caitlin Morrison, 'EU cracks down on Airbnb with demands for change in pricing and refund policy' (*Independent*, 16 July 2018) <https://www.independent.co.uk/news/business/news/airbnb-price-refund-policy-eu-compensation-claims-european-commission-a8449546.html> accessed 5 April 2023.

Jon Porter, 'EU forces Amazon to make it easier to cancel Prime subscriptions in Europe' (*Verge*, 5 July 2022) <EU forces Amazon to make it easier to cancel Prime subscriptions in Europe> accessed 5 April 2023.

European data protection board, 'EDPB publishes three guidelines following public consultation' (*European Data Protection Board*, 24 February 2023) <https://edpb.europa.eu/news/news/2023/edpb-publishes-three-guidelines-following-public-consultation_en> accessed 5 April 2023.

European commission, 'Digital fairness – fitness check on EU consumer law' (*European Commission*, 17 May 2022) <https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13413-Digital-fairness-fitness-check-on-EU-consumer-law_en> accessed 5 April 2023.

Luca Bertuzzi, 'Dark patterns, online ads will be potential targets for the next Commission, Reynders says' (*Euractiv*, 12 December 2022) <https://www.euractiv.com/section/digital/interview/dark-patterns-online-ads-will-be-potential-targets-for-the-next-commission-reynders-says/> accessed 5 April 2023.

Nerdwriter1, 'How Dark Patterns Trick You Online' (*YouTube*, 29 March 2018) <https://www.youtube.com/watch?v=kxkrdLI6e6M> accessed 5 April 2023.

Xigen, 'The Dark Patterns Report' (*Xigen*) <https://xigen.co.uk/reports/the-dark-patterns-report/> accessed 5 April 2023.

Caroline Sinders, 'What's In a Name? Unpacking Dark Patterns versus Deceptive Design' (*Medium*, 18 June 2022) <https://medium.com/@carolinesinders/whats-in-a-name-unpacking-dark-patterns-versus-deceptive-design-e96068627ec4> accessed 5 April 2023.

Todd Libby, 'Enough with "Dark Patterns" Already! This Isn't Going To Go Over Well' (*Todd Libby*, 1 January 2023) <https://toddl.dev/posts/enough-with-dark-patterns-already/> accessed 5 April 2023.

Amy Hupe, 'Why it's time to update our language about bad design patterns' (*Amy Hupe*, 1 July 2022) <https://amyhupe.co.uk/articles/changing-our-language-on-bad-patterns/> accessed 5 April 2023.

Jennifer Riggins, 'Critics of ‘Deceptive Design’ Push for a More Ethical UX' (*The New Stack*, 11 March 2022) <https://thenewstack.io/critics-of-deceptive-design-push-for-a-more-ethical-ux/> accessed 5 April 2023.

System Concepts, 'Persuasive design vs dark patterns: Where to draw the line' (*System Concepts*, .) <https://www.system-concepts.com/insights/persuasive-design-vs-dark-patterns/> accessed 5 April 2023.

Laura Lugo, 'Deceptive Design and how to avoid dark patterns' (*Bootcamp, Medium*, 30 June 2022) <https://bootcamp.uxdesign.cc/deceptive-design-and-how-to-avoid-dark-patterns-62a6dff026e4> accessed 5 April 2023.

Harry Brignull, 'About this site' (*Deceptive Design*) <https://www.deceptive.design/about-us> accessed 5 April 2023.

Catalina Coanta and Cristiana Santos, 'Dark Patterns Everything: An Update on a Regulatory Global Movement' [2023] Network Law Review <https://www.networklawreview.org/digiconsumers-two/> accessed 28 May 2023.

Yashasvi Nagda, 'What is Darkness in Dark Patterns?' (Medium (Muzli - Design Inspiration), 17 March 2020) <https://medium.muz.li/what-is-darkness-in-dark-patterns-e981465c0c57> accessed 28 May 2023.

Adam Hayes, 'What Is a Red Flag? Definition, Use in Investing, and Examples' (*Investopedia*, 25 March 2022) <https://www.investopedia.com/terms/r/redflag.asp> accessed 28 May 2023.

Nick Killick, ' From Red to Green Flags' (*IHRB*, 2 May 2011) <https://www.ihrb.org/focus-areas/commodities/commentary-red-green-flags-corporate-responsibility> accessed 28 May 2023.